07.02.2020

Towards the European Level Exchange of Facial Images

Legal Analysis for TELEFI project

Riigihange "Näokujutiste hõivamise ja kasutamisega seotud juriidiliste regulatsioonide analüüs EL liikmesriikides"

Riigihanke viitenumber 208411

Table of Contents

INTRODUCTION

People's facial images constitute biometric data: they are more or less unique, cannot be changed, and cannot easily be hidden.[1] Pursuant to the globalisation of the economy and the internationalisation of companies, the activities of different persons have increasing cross-border effects. Rapid technological developments and globalization have introduced new challenges to the protection of personal data. The scale of the collection and distribution of personal data has increased significally. Fast-evolving technology allows a person to be identified for private or public purposes by at least the following methods:

1) Facial recognition
2) Gait analysis
3) Body size/shape/proportion detection
4) Voice, pitch, tone, language, dialect, accent, etc.
5) Chemical/biological/medical analysis (e.g., breath composition, breathing rate, pulse, blood pressure, electro-galvanic skin properties)
6) Special characteristics (e.g., scars, injuries, tattoos, piercings)
7) Corrective/enhancement technology (currently glasses, lenses, hearing aids, etc. but tecnology is developing in time)
8) Unique biometric identification where available (e.g., retina patterns, 'conventional' fingerprints, DNA)[2]

There will definitely be more technological methods in the future. In addition, technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[3] Thus, public authorities are of the opinion that for enhancing the provision of security, including preventing the use of double identities, preventing crime, conducting criminal investigations and other potential new

[1] European Union Agency For Fundamental Rights. FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement. 27 November 2019. Online available: https://fra.europa.eu/en/publication/2019/facial-recognition (28.11.2019).

[2] Vic Grout. No More Privacy Any More? Published 01 January 2019. Online available: https://www.mdpi.com/2078-2489/10/1/19/htm (31.10.2019).

[3] Recital 3 of the Directive (EU) 2016/680.

applications (e.g., fully automated border control), the (electronic) methods for the identification of individuals or the verification of their identity need to be updated constantly.[4]

Having no biometric data exchange between countries poses the risk that double identities could be created and identity documents or another person's identity used unlawfully. In addition, it could also prevent the performance of obligations under international agreements.[5]

The application of modern biometric comparison methods could reduce the potential for the creation of double identities and increase the likelihood of identifying instances of unlawful usage. Clear identification and effective background checking solutions would increase the certainty that an electronic identity has been created for an identified individual and is clearly tied to the physical identity of the person.[6]

Therefore, it appears essential for legislators to catch up with current trends, as the technology of biometric systems has developed rapidly in recent years and is now finding its practical use more than before.

DNA profiles, fingerprints and vehicle registration data are currently exchanged within the PRÜM framework[7] in the EU for combating cross-border crime, terrorism and illegal migration. The PRÜM system has been successfully employed for many years and has reached a point where the introduction of new modalities, including facial images, is being considered.[8]

The European Union (EU) funded project *Towards the European Level Exchange of Facial Images* (hereinafter referred to as 'TELEFI project') conducts a study on how facial recognition is being used for the investigation of crime across the Member States of the European Union.[9]

[4] Siseministeerium, Biomeetriliste andmete kasutamise kontseptsioon. Online available: https://adr.siseministeerium.ee/sisemin/dokument/907446 (31.10.2019).
[5] Siseministeerium, Op.Cit.
[6] Siseministeerium, Op.Cit.
[7] Note: Article 61 of Directive (EU) 2016/680 states that international agreements involving the transfer of personal data to third countries or international organisations, which were collected by Member States prior to 6 May 2016 and which comply with EU law as applicable prior to that date, shall remain in force until amended, replaced or revoked.
[8] About TELEFI project. Online available: https://www.telefi-project.eu/telefi-project/about-telefi-project (15.10.2019).
[9] About TELEFI project. Op.cit.

The key focus of the TELEFI project is the use of facial recognition in criminal investigations. However, information is also collected on other databases containing facial images (relating to personal identity and driving) with the purpose of obtaining a complete overview of the field. This will provide a future opportunity to consider the legal cross-use of these additional databases for criminal investigations/proceedings and transnational data exchange.[10]

Ernst & Young Baltic AS (hereinafter also referred to as 'EY' or 'we') has been chosen by the Estonian Forensic Science Institute to provide the analysis of legal regulations in various Member States as one part of the TELEFI project.

As stated on the TELEFI project website, the full report of the whole TELEFI project will be published at the end of the TELEFI project, containing a detailed description of the current status of facial recognition across EU Member States as well as recommendations on harmonising the field across Europe. In addition, a dissemination conference will be held to provide a platform for sharing the TELEFI results and stimulating discussion on the way forward.[11]

As requested by the Estonian Forensic Science Institute in its public procurement, in the following legal analysis, we address the following legal questions as one part of the whole TELEFI project:

1) Comprehensive overview of the laws of EU Member States regarding offence proceedings, which regulate the collection and use of facial images.
2) Comprehensive overview of the laws of EU Member States regarding the detention of persons, which regulate the collection and use of facial images.
3) Exhaustive overview of the laws of EU Member States regulating the issuance and use of identity documents (passport, identity card, driving licence), which regulate the collection and use of facial images.
4) Exhaustive overview of the laws of EU Member States regulating the collection and use of facial images by the state (government entity), which are not listed in points 1-3.
5) Comprehensive overview of whom (which groups of natural persons) facial images are collected from according to the abovementioned laws of EU Member States.
6) Comprehensive overview for what purposes it is allowed to use facial images collected according to the abovementioned laws of EU Member States.

[10] About TELEFI project. Op.cit.
[11] About TELEFI project. Op.cit.

7) In which databases, according to the abovementioned laws, these facial images are stored and processed and which laws of EU Member States regulate the establishment of such databases.
8) Whether the laws of the EU Member State allow the use of data, including facial images, which have been collected for civil purposes to be used in offence proceedings?
9) Whether the laws of the EU Member State allow the use of facial images collected in that Member State to be used by other countries (government entities) for the purpose of offence proceedings in these countries? In other words, is cross-border cooperation possible between the countries (government entities)?

The legal analysis is divided into four chapters. The structure of this legal analysis has been determined by the main research questions and their mutual connections in legal framework in the EU applicable to all Member States.

In the first chapter of the analysis we will focus on legal notions and definitions, as the legal framework seems rather hectic and complex for EU Member States in the context of personal data protection for law enforcement purposes. There appears to be lots of mixed terminology in this sphere, which may need clarification in future law-making in both: in the EU and in Member States level.

The second chapter of the current analysis is concentrated on the legal intruments of the EU and Council of Europe, which are either directly or non-directly applicable in all EU Member States. Thus, it is also important for EU Member States to understand that EU law regulates the collection and use of facial images under the EU data protection *acquis.*

The third chapter focuses on national (domestic) laws found in EU Member States regarding the main legal questions stated by the Estonian Forensic Science Institute in current public procurement procedure.

The fourth chapter of this analysis is focused on the so-called cross-use of biometric data and some ethical considerations for further developments in this area in law-making, as facial images are unique biometric identifiers under EU law.

In this legal analysis, we have mostly used the historical, systematic, analytical and comparative method. In addition, as for an empirical study, we have made surveys and interviews with specialists and experts in this field.

In compiling the legal analysis, we have mainly used foreign legal acts and literature. The sources on the given subject are rather scarce and mostly in languages we do not master. Nevertheless, the works of the internationally recognised scientists and jurists such as Kindt, Jasserand-Breeman, etc., have largely been used. Articles on the given subject have been used, including works published in magazines of a legal and sometimes technological nature. Reports, explanatory notes, etc. compiled by international cooperation bodies and expert groups, such as the Working Party of Article 29 of General Data Protection Regulation, European Union Agency For Fundamental Rights (FRA), national experts for TELEFI project, have also been used. When clarifying legal problems related to the topic, we have also relied on explanatory reports and selected decisions of various courts of the Member States of the EU, European Court of Human Rights and the European Union Court of Justice in the given research field. However, accessing certain Member States' legal regulations and court cases on the given subject was practically impossible because of the non-existence of relevant national laws, data, registers or relevant contact persons and lack of access to highly sensitive information (considered national or state secrets).

The main EU law source – Directive (EU) 2016/680 – and the main legal acts of EU Member States in this field, which should be compliant with said Directive, have mainly been used as reference and/or comparative objects in order to benchmark the current status.

Pursuant to the volume limitations, and the nature and aim of the current legal analysis in this public procurement, it has not been possible to deal with all the legal questions or legal problems related to special categories of personal data, biometric data, facial images and facial recognition because this field is rather innovative and rapidly changing making it impossible even for legal scholars to be up to date.

The legal analysis does not cover matters related to specific technology, risk analysis, economic impact or technological infrastructure.

In the current legal analysis, legal instruments have been used in the wording as at 31 October 2019 at the latest. Thus, the latest developments in the jurisdictions concerned have not been checked and therefore, the report is not suitable for reliance. The legal analysis is based on the wording of legislation available and other materials in force at the time of performing this legal analysis. Given the scope of

agreement between you and Ernst & Young Baltic AS and the work methodology applied, the deliverable has not been reviewed by legal professionals in jurisdictions concerned.

Not all legislation and other materials used have official English translations and we have therefore used the unofficial translations available online or translated the materials ourselves as necessary. We assume no responsibility for the compliance of such translations with any official translations that may be published later. Thus, we assume no responsibility for the compliance of terms, notions, legal definitions translated into English from national laws, which might differ in practice and not be comparable to make comprehensive conclusions.

This legal analysis is prepared for the Estonian Forensic Science Institute as our client, subject to the terms and conditions of our agreement. It is not to be relied upon by any other person. In no event is Ernst & Young Baltic AS liable for any losses, damages or expenses sustained as a result of the reliance by such party on this advice. Furthermore, this legal analysis is based on the facts provided to us as set out above and on the law as promulgated on the date (31 October 2019) of this legal analysis. We do not take any responsibility for advising on any changes to our legal analysis which may arise as a result of subsequent changes in law or practice. It is our standard policy that we will not accept liability in the event of any claim or allegation of negligence on our part for an amount in excess of the fee charged for the services giving rise to the opinion upon which such claim is based. Our legal analysis is based on the technical terms provided by the Estonian Forensic Science Institute for this current public procurement. **We have not sought to establish the reliability of the information given to us.**

SUMMARY

Privacy is like freedom: you do not recognize its importance until it is taken away.[12]

It appears that until the adoption of the new data protection framework in the EU (Data Protection Reform Package), the notion of 'biometric data' had not been officially introduced in any EU data protection legislation. Thus, it is a completely new notion.

[12] D. Flaherty. On the Utility of Constitutional Rights to Privacy and Data Protection. Case W. Res. L.Rev., 1990-1991, p. 831.

There are major differences among the definitions used at the EU level, especially in regard to the technical process of extraction of biometric information and its transformation into a digital template. None of these definitions refers to the automatic process that allows the identification of individuals or the verification of their identity.

The legal definition proposed by European institutions for the term 'biometric data' appears to be incomplete. There may be other opinions by legal scholars and there are definitely a variety of notions and terms used in the national laws of EU Member States, making it difficult to understand and compare legal regulations.

According to Article 3 (13) of Directive (EU) 2016/680, 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Biometric characteristics are not themselves considered biometric data. Only the personal data 'resulting' from their processing qualify as biometric data. Thus, it is not the face of an individual, but the images of their face (photographs) that would be classified as biometric data. Likewise, it is not their fingertip, but a fingerprint image that will be classified as biometric data. As legally defined in Article 10 (1) and Article 3 (13) of the Directive 2016/680, 'biometric data' are first of all 'personal data'. To be protected under the data protection rules, personal data need to be, at least, part of a 'filing system' or 'processed'. The biometric characteristics themselves cannot be processed. Only the data generated from these characteristics can. From a legal point of view, it is absolutely not clear what this 'specific technical processing' comprises.

From a legal point of view, Recital 51 of the General Data Protection Regulation (EU Regulation 2016/679 or 'GDPR') makes a distinction between the legal nature of simple 'photographs' and biometric 'facial images'. However, it should be stressed that the GDPR does not apply in the field of law enforcement as this is governed by another EU legal instrument – Directive (EU) 2016/680.

There appears to be general uncertainity in EU Member States about the qualification of facial image data as biometric data.

There is no legal definition prescribed by EU legislation on what a facial image is and what facial recognition is in regard to the processing of personal data for law enforcement purposes within the meaning of Directive (EU) 2016/680, as the GDPR Article 29 Data Protection Working Party (2012) definition cannot be used for that public purpose. There is no specific EU legal framework which governs the processing of biometric data, including facial images and what can be considered facial recognition from a clear legal point of view for the purposes laid down in Directive (EU) 2016/680.

The main EU legal instrument in the field of data protection for police and criminal justice authorities is Directive (EU) 2016/680. It is not directly applicable to Members States, and its provisions had to be transposed into national laws by Member States on 6 May 2018 at the latest. It should also be noted that Directive (EU) 2016/680 is a 'minimum harmonisation' Directive, leaving non-harmonised areas of the Directive to the discretion of Member States.

It should be noted that if EU institutions have regulated specific legal matters with the special legal instrument – Regulation – at the EU level, this Regulation is directly applicable to EU Member States. Thus, additional national law-making by Member States is not needed in the given legal matter and is even prohibited.

If specific legal matters are regulated with the legal instrument – Directive – at the EU level, this Directive in general is not directly applicable to Member States. Thus, additional law-making by Member States in national laws is highly required, as the Directive must be adopted/transposed to national laws within the specific period of time specified in the Directive.

The following key points are relevant in EU law on data protection in police and criminal justice matters:

- Within the EU, data protection in the police and criminal justice sector is regulated in the context of both national and cross-border processing by police and criminal justice authorities of the Member States and EU actors.
- At the Member State level, Directive (EU) 2016/680 needs to be incorporated into Member State national law.
- Specific legal instruments govern data protection in police and law enforcement cross-border cooperation, particularly in combating terrorism and cross-border crime.
- Special data protection rules exist for the European Police Office (Europol), the EU Judicial cooperation unit (Eurojust) and the newly established European Public Prosecutor's Office, which are all EU bodies assisting and promoting cross-border law enforcement.

- Special data protection rules also exist for the joint information systems that have been established at the EU level for cross-border information exchange between the competent police and judicial authorities. Important examples are the Schengen Information System II (SIS II), the Visa Information System (VIS) and Eurodac, a centralised system containing the fingerprint data of third-country nationals and stateless persons applying for asylum in one of the EU Member States.
- **The EU is still in the process of updating the data protection provisions so as to be in line with the provisions of Directive (EU) 2016/680. The latter most likely means that the laws of Member States in this particular area are not yet in line with EU legal framework on data protection.**

One important distinction between Council of Europe and EU law is that CoE law, unlike EU law, also applies to the national security area. This means that Contracting Parties (Member States) need to stay within the remit of Article 8 of the European Convention on Human Rights even for activities related to national security:

- The Modernised Convention 108 and the CoE Police Recommendation apply to data protection across all areas of police work.
- The Cybercrime Convention (Budapest Convention) is a binding international legal instrument dealing with crimes committed against and by means of electronic networks. It is also relevant for the investigation of non-cyber-crimes that involve electronic evidence.

As to national laws of Member States, the right to one's own image exists in several countries, including Belgium, where it has been created by case law. The right protects one's image as well as, according to some, one's behavior. The right is based on a so-called 'personality' right to one's image. It is a so-called ultimate right and can be limited only with specific legislation.

In order to collect and use biometric data, including facial images, there should be valid legal basis. In some cases (for instance so-called automated facial recognition), a substantial impact assessment by legislator must be done before establishing special legal provisions for data processing and means to protect a person's privacy. Processing of biometric data in various proceedings in one consolidated database is subject to the principles of personal data protection (i.e. purpose limitation, legality, data minimisation, transparency, retention limitation, application of appropriate safeguards). In any case, a valid legal basis for processing biometric data for specific purposes must exist.

Laws on biometric data, which also regulate the collection and use of facial images in offence proceedings in EU Member States, are in force only in Latvia. It appears that other EU Member States have different approaches towards law-making. Thus, having laws in place on offence proceedings such as Criminal Codes, Criminal Procedure Acts and Personal Data Protection Acts, where the collection and use of facial images (namely 'photographs') are regulated as part or components of offence proceedings. Special law only on facial images collection, use or processing as *per se* for the purpose of law enforcement does not exist.

It appears that legal acts regarding the detention of persons, which regulate the collection and use of facial images, are mostly laws and regulations related to imprisonment and execution of detention, such as Criminal Procedure Acts. It appears that Member States make a distinction between data subject categories. However, categorisation appears to be based on characteristics of persons, not on characteristics of biometric data.

At the EU level, the legal basis for collecting biometric data (facial image and two fingerprints taken flat) has been established by Regulation (EC) No. 2252/2004 of the European Parliament and the Council and Council Regulation (EC) No. 444/2009 amending it.[13] This Regulation is directly applicable in all EU Member States. However, it appears that in most EU Member States personal identification documents are also regulated by national laws (mostly in Acts, sometimes mentioned in Regulations) and a photo of the person is required on the person's identity document. Biometric data is collected for the purpose of processing it in the procedure for issuance of passports, ID cards and travel documents. The Member State is required to collect biometric data for this purpose. In general, any other use or storage of the personal data collected for the purpose of issuance documents in accordance with national legislation is not prohibited by national laws. However, in general, national laws also provide no legal basis for such actions, meaning that processing this personal data for any other purposes is allowed if the legal basis for it has been provided in other (national) legal acts. In any case, a valid legal basis for processing biometric data for specific purposes must exist.

Before establishing a legal basis under EU or national law for processing biometric data, the legislator must perform a balancing test, as data processing must be proportionate to the purpose pursued; data

[13] REGULATION (EC) No 444/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Online available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF.

processing must respect the genesis and principles of data protection law; appropriate and specific means must be ensured for the protection of the fundamental rights and interests of the data subject.

By other national laws regulating the collection and use of facial images by Member States (government entities), it appears that these are mostly related to immigration matters, aliens (foreigners, refugees) and personal data processing (on GDPR grounds). Poland has also listed the Labour Code and Sweden the Law on Camera Surveillance.

As for collection of facial images, it appears that facial images (photographs) are collected mostly from citizens for issuance of their identification document and from suspects, accused and prisoners.

In general, the main purpose of using and collecting facial images is identification and the prevention and investigation of crimes.

The main databases according to the laws of different Member States in which facial images are stored and collected, are mostly related to law enforcement agencies, border control and identification documents.

In most proceedings regulated by EU law, Member States are obliged to collect biometric data and transfer it to central EU databases. Data comparison is often voluntary (and depends on the necessity evaluated by the responsible authority), as is data collection from EU databases for investigation, detection and prosecution in criminal offences.

In most cases, Member States' laws allow use of personal data, including facial images, that has been collected for other (civil) purposes in offence proceedings. However, Austria and Luxembourg do not allow data collected for other (civil) purposes to be used in offence proceedings.

Regarding laws allowing the use of facial images collected in a particular Member State to be used by other Member States (by the government entities) for the purpose of offence proceedings in these Member States it appears to be possible. In other words, cross-border cooperation on justice and crime matters should most likely be possible between Member States (between government entities).

It appears that in most EU Member States the collection and use of biometric data, including facial images and automatic or live facial recognition in offence/criminal proceedings is not literally (word-by-word) stipulated, which makes it rather difficult to find relevant provisions in regulating the topic.

It appears that the quality and quantity of legal provisions related to facial images varies among EU Member States. There are some EU Member States which might be considered as more advanced in terms of regulation of facial images than the others.

Based on the technological neutrality principle, the requirements for software and hardware are established in laws only as general requirements without specifying technical details or technical requirements for systems.

It appears that in most EU Member States, legal basis for establishing one exhaustive database for biometric data, including facial images, is not in place.

There is no legal definition for the so-called cross-use of personal data. Cross-use of data is generally restricted by the principle of purpose limitation, i.e biometric data can only be processed for other purposes, if the purposes of such further processing are compliant with the purposes of its initial collection. If further processing is not compliant with the purposes of its initial collection and use, a specific separate legal basis for such further processing must be created by law (or the consent of the data subject).

Further processing of personal data received from EU central databases is prohibited or permitted only to a limited extent and for specific reasons established under the respective EU laws. This applies to the transfer of such personal data to third countries, international organisations and other (private) persons.

The scenario of law enforcement access to personal data initially collected for a different purpose (commercial, operational) from private parties raises complex issues, and Directive (EU) 2016/680 lacks the essential provisions to ensure the protection of individuals' right to data protection. If there is uncertaintity surrounding the applicable rules at the EU level, then there is uncertainty surrounding interpretations at the national level, causing a likelihood of diversions. Personal data, including biometric data, collected for a specific purpose should be used for compatible purposes or further processed under a separate legal basis.

It appears that there is some ambiguity in Article 4 of Directive (EU) 2016/680. Article 4(2) of Directive (EU) 2016/680 does not state whether the initial purpose falls within or outside the scope of Directive (EU) 2016/680, nor does it discuss the further processing of personal data. According to Dr Jasserand-Breeman, Article 4(2) of Directive (EU) 2016/680 only sets out the conditions under which further processing for a purpose other than the original purpose of collection is allowed.

Not providing a specific legal basis for the subsequent processing of GDPR data in a law enforcement context definitely creates further problems. The topic has been left in the hands of Member States and their national courts until it gets challenged before the CJEU.

The practices and purposes of using facial images as one component in biometric data vary significantly between continents (Europe, USA, Asia) and EU Member States depending on the national legal framework, the maturity of the Member State being part of the EU, social and geopolitical trends and the level of technological development as well as the R&D level in the specific region or state.

It appears that using facial images, fingerprints, DNA etc. has always been important in policy-making and it is the task of law enforcement authorities. It is of public interest that such images are used to prevent, detect and prosecute crime upon the conditions that there is a clear legal framework and that any use, including storage, is proportionate.[14]

Only when transparent legal framework exists can law enforcement authorities be entitled to identify suspects based on images contained in, for example, CCTV[15] footage registering a crime, and compare these with databases of previously convicted criminals or (arrested) suspects.[16]

Facial images are a powerful new biometric, but the acceptance by the public of their use for crime control purposes may depend on the extent to which governance arrangements provide assurance that their use will be in the public interest and intrusion into individual privacy controlled and proportionate.[17]

[14] E. J. Kindt. Having yes, using no? About the new legal regime for biometric data. Computer Law and Security Review Volume 34, Issue 3, June 2018, pp 523-538.
[15] Closed Circuit TV. A self-contained surveillance system comprising cameras, recorders and displays for monitoring activities in a store or company. Online available: https://www.pcmag.com/encyclopedia/term/59748/cctv, accessed 31.10.2019.
[16] E. J. Kindt. Having yes, using no? About the new legal regime for biometric data. Op.cit.
[17] Biometrics strategy and forensic services, fifth Report of Session 2017–19. House of Commons Science and Technology Committee. Published on 25 May 2018. Online available: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf, accessed 19.11.2019.

In order to facilitate the debate on the use of facial images (or biometric systems in general), including analysis of legal framework, a sound joint understanding of the legal notions and legal terminology and technical functioning of biometric systems and their main and technical features is highly required before substantial law-making or harmonisation at the EU level.

1 TERMS AND NOTIONS RELATED TO BIOMETRIC DATA incl FACIAL IMAGES

1.1. Biometric data

EU law considers people's facial images, which are a form of biometric data, 'sensitive data' to be protected as a fundamental human right to one's privacy.

Dr Kindt has heavily criticised different definitions of 'biometric data'[18] and proposed the following working definition of 'biometric data' in year 2013: *"All personal data which (a) relate directly or indirectly to unique or distinctive biological or behavioral characteristics of human beings and (b) are used or are fit to be used by automated means (c) for purposes of identification, identity verification or verification of a claim of living natural persons."*[19]

It appears that until the adoption of the new data protection framework in the EU (Data Protection Reform Package), the notion of 'biometric data' had not been officially introduced in any EU data protection legislation. Thus, it is a completely new notion.[20]

In addition, there appears to be great deal of confusion as to what exactly has been defined so far by whom and what exactly consists of what for legislators in Member States to transpose proper definitions with proper meaning into their national legislation, if needed. How are terms under consideration related to and positioned with each other, if at all?

Dr Jasserand-Breeman has found **five definitions of biometric data** stipulated by different European bodies/institutions:

[18] E. J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis. Springer, 2013, p 154-155.
[19] E. J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis. Springer, 2013, p 149.
[20] C. Jasserand-Breeman. (2019). Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?. Groningen, University of Groningen, p 21-22.

European bodies/institutions	Definitions of 'biometric data'
Article 29 Working Party and EDPS	Biological properties, physiological characteristics, living traits, or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. (*Opinion 4/2007), Definition quoted by the EDPS in Opinion on the Turbine Project (2011).*
PACE	Unique physical and behavioural characteristics that differ from one human being to another and that remain, in most cases, unaltered for life. *(Haibach report, 2011)*
Consultative Committee of Convention 108	Data resulting from a specific technical processing of data concerning the physical, biological, or physiological characteristics of an individual which allows the unique identification of the latter. *(Draft explanatory report of the modernized version of Convention 108, 10 July 2013)*
European Commission and European Parliament	***Any personal*** data relating to the physical, physiological, or behavioural characteristics of an individual which allow their unique identification, **such as facial images**, or dactyloscopic data. **(Text "Any personal" added by the European Parliament indicated in italic.)** *(Article 4(11) of the proposed General Data Protection Regulation and* ***Article 3(11) of the proposed Directive on data retention and law enforcement, 2012)*** *(Resolutions of 12 March 2014 on two proposals of the European Commission)*

European Commission and Council of the EU	***Any personal*** data ***resulting from specific technical processing*** relating to the physical, physiological, or behavioural characteristics of an individual, which ***allows or confirms the*** unique identification of ***that*** individual, such as facial images, or dactyloscopic data. **Text added by the European Parliament indicated in italic.)** *(Article 4(11) of the proposed General Data Protection Regulation) (Political agreement of 15 June 2015 on the General Data Protection Regulation)*

As you can see from this table, **there is a major difference between definitions, especially in regard to the technical process of extraction of biometric information and its transformation into a digital template.** None of these definitions refers to the **automatic process** that allows the identification of individuals or the verification of their identity.[21]

The legal definition proposed by the European institutions for the term 'biometric data' appears to be incomplete. Dr Jasserand-Breeman proposes that the legal definition of 'biometric data' should remain **technologically neutral** and not mention any format or the technical processing of data.[22] She also notes that in the absence of adaptation of the Data Protection Reform Package (negotiations pending), **the legal definition that prevails for the time being at the EU level is the one provided by the Article 29 Working Party.[23] There may be other opinions by legal scholars and there are definitely different notions and terms used in the national laws of Member States.**

According to Article 3 (13) of Directive (EU) 2016/680 (hereinafter also referred to as 'Law Enforcement Directive' or 'Police Directive' or 'Data Protection Directive for Police and Criminal Justice Authorities'), **'biometric data'** means **personal data resulting from specific technical processing** relating to the **physical,** physiological or behavioural characteristics of a natural person, which **allow or confirm** the **unique identification** of **that natural person**, **such as facial images or dactyloscopic data.**

[21] C. Jasserand-Breeman. (2019). Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?. Groningen, University of Groningen, p 52-53.
[22] C, Jasserand-Breeman. (2019). Op.cit. p 53.
[23] C. Jasserand-Breeman. (2019). Op.cit. p 53.

Thus, as described by the European Union Agency For Fundamental Rights[24], there appears to be **two categories of information as biometric data**:

1) 'Physical/physiological characteristics', which pertain to bodily characteristics, such as facial features, fingerprints, weight, retina and iris characteristics.

2) 'Behavioural characteristics', such as deeply ingrained habits, actions, personally traits, addictions, etc.[25] This includes behavioural characteristics that could permit the unique identification of a person, such as hand-written signature or a way of walking or moving.[26]

From a legal point of view, it is not entirely clear what this 'specific technical processing' consists of. Dr Jasserand-Breeman has described the technical steps of biometric recognition in her doctoral thesis in detail. She is of the opinion that some authors as well as the Article 29 Working Party incorrectly use the phrase 'raw (biometric) data' to designate a biometric sample. Raw (biometric) data are, for example, a fingerprint, fingertip, iris, voice, etc. **In the absence of any technical processing through which raw data are obtained, these fall outside the scope of biometric data.** In her opinion the term 'raw data' should only be used as synonym of biometric characteristics.[27]

Dr Jasserand-Breeman states that biometric characteristics are not themselves considered biometric data. **Only the personal data 'resulting' from their processing qualify as biometric data.** Thus, it is not the face of an individual, but the images of their face (pictures) that would be classified as biometric data. Likewise, it is not their fingertip, but a fingerprint image that will be classified as biometric data. As legally defined, 'biometric data' are first of all 'personal data'. To be protected under data protection rules, personal data need to be, at least, part of a 'filing system' or processed by automatic means. **The biometric characteristics themselves cannot be processed. Only the data generated from these characteristics can.**[28]

[24] FRA-European Union Agency for Fundamental Rights, Facial recognition technology:
fundamental rights considerations in the context of law enforcement, published 27.11.2019, page 5.

[25] Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, WP 193, Brussels, 27 April 2012, p 4; See also: P. Misra. (2018). Here's how face recognition tech can be GDPR compliant. Online available: https://thenextweb.com/contributors/2018/10/29/heres-how-face-recognition-tech-can-be-gdpr-compliant/, accessed 15.11.2019.

[26] FRA-European Union Agency for Fundamental Rights. Op.cit., page 5.

[27] C. Jasserand-Breeman. (2019). Op.cit. p 67.

[28] C. Jasserand-Breeman. (2019). Op.cit. p 72.

1.2. Facial images and facial recognition

According to the definition stated in the European Commission Impact Assessment Report a photo is the image of a person on a substrate (paper, plastic) and a **facial image is the digital representation of the image of a person**. [29]

Dr Kindt is of the opinion that **facial images could be described as images taken of the face** (and sometimes shoulders), in particular, of persons, **whether analogue or digital**, consisting of single picture(s) or moving ones (e.g. video images).[30]

According to dr Jasserand-Breeman **not all photographs will qualify as 'biometric data'**, but only those that 'allow the unique identification or authenticate' an individual.[31] **To determine whether a facial image is fit for biometric recognition, different factors or parameters should be taken into account,** such as light, exposure, location or the resolution of the camera.[32] These parameters are linked to technological developments in face recognition.

According to European Union Agency For Fundamental Rights, **digital facial images belong to the 'physical/physiological characteristics' of the information as 'biometric data'**.[33] However, based on Dr Kindt's comparative research on Belgium, France and the Netherlands, **there appears to be general uncertainty among EU Member States on the qualification of facial image data as biometric data**.[34]

From a legal point of view, Recital 51 of the **GDPR makes a distinction between the legal nature of simple 'photographs' and biometric 'facial images'. However, it should be stressed that GDPR does not apply in the field of law enforcement, as this area is governed by another EU legal instrument – Directive 2016/280.** The definition of biometric data according to Recital 51 of the GDPR applies to photographs

[29] European Commission Impact Assessment Report on the establishment of an EU Entry Exit System. Brussels, 6.4.2016. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0115&qid=1573980037866&from=EN (27.11.2019)

[30] Kindt Els, Doctoral thesis 'The processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a Legal framework', Katholieke Univerisiteit Leuven 2012, p 89 ff. Online available: https://lirias.kuleuven.be/bitstream/123456789/345184/1/PH_D_text_PartI%2BPartII_17.04-Pservice.pdf, accessed 20.11.2019.

[31] C. Jasserand-Breeman, (2019). Op. cit, p 72-73.

[32] See for instance opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012, given by The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, online available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf (14.10.2019).

[33] FRA-European Union Agency for Fundamental Rights. Op.cit., page 5.

[34] E. J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis. Springer, 2013, pp 160-164.

only when these are processed through specific technical means allowing the unique identification or authentication of a natural person.

There is no legal definition prescribed by EU legislation on what a facial image is in regards to the processing of personal data for law enforcement purposes within the meaning of Directive (EU) 2016/680.

Just to add as a comparison from the private sector for this topic, according to opinion No. 02/2012 of the special Working Party on GDPR[35] on facial recognition in online and mobile services the **definition of facial recognition** is the **automatic processing of digital images**, which *contain* the faces of individuals for the purpose of identification, authentication/verification **or** categorisation of those individuals.[36]

The process of facial recognition in online and mobile services comprises a number of discrete sub-processes, as follows:[37]

1) Image acquisition: The process of capturing the face of an individual and converting it to a digital form (the digital image is a representation of a two-dimensional image in a digital form). However, recent advances in facial recognition technology require that three-dimensional images are included in addition to both static and moving images (i.e. photographs, recorded and live video). In an online or mobile service, the image may have been acquired in a different system, e.g. taking a photograph with a digital camera which is then transferred to an online service.

2) Face detection: The process of detecting the presence of a face within a digital image and marking the area.

3) Normalisation: The process of smoothing variations across detected facial regions, e.g. converting to a standard size, rotating or aligning colour distributions.

4) Feature extraction: The process of isolating and outputting repeatable and distinctive readings from the digital image of an individual. Feature extraction can be holistic, feature-based or a combination of the two methods. The set of key features may be stored for later comparison in a reference template.

---

[35] Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[36] Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012, given by The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, online available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, accessed 14.10.2019.

[37] Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012, given by The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, online available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, accessed 14.10.2019.

5) Enrolment: If this is the first time an individual has encountered the facial recognition system, the image and/or reference template may be stored as a record for later comparison.

6) Comparison: The process of measuring the similarity between a set of features (the sample) with one previously enrolled in the system. The main purposes of comparison are identification and authentication/verification. A third purpose of comparison is categorisation, which is the process of extracting features from an image of an individual in order to classify that individual in one or several broad categories (e.g. age, sex, colour of clothes, etc). It is not necessary for a categorisation system to have an enrolment process.[38]

However, it should be stressed again that GDPR does not apply in the field of law enforcement as this area is governed by another EU legal instrument – Directive 2016/280.

There is no legal definition prescribed by EU legislation of facial recognition in regard to the processing of personal data for law enforcement purposes within the meaning of Directive (EU) 2016/680, as the GDPR Article 29 Data Protection Working Party (2012) definition cannot be used for that public purpose. There is no specific EU legal framework which governs the processing of biometric data, including facial images and what can be considered facial recognition from a clear legal point of view for the purposes laid down in Directive (EU) 2016/680.

2. LEGAL FRAMEWORK APPLICABLE TO ALL EU MEMBER STATES

2.1 Legal instruments of the European Union

In order to balance the individual's interests in data protection and society's interests in data collection for the sake of fighting crime and ensuring national and public safety, the Council of Europe and the European Union have historically enacted specific legal instruments.[39]

[38] Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012, given by The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, online available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, accessed 14.10.2019.

[39] Handbook on European data protection law 2018 edition. Online available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, accessed 13.11.2019.

Thus, in order to understand what the legislators in all EU Member States have to understand, interpret or transpose into their national laws, we hereby need to describe in general the historic and current European Union (EU) legal instruments:

1. **Directive (EU) 2016/680[40] (also by some authors called the 'Law Enforcement Directive' or 'Police Directive' or 'Data Protection Directive for Police and Criminal Justice Authorities').**

This directive **is not directly applicable to Member States** and its provisions had to be transposed into national laws by Member States on 6 May 2018 at the latest. **It should also be noted that Directive (EU) 2016/680 is a 'minimum harmonisation' Directive, leaving non-harmonised areas of the Directive to the discretion of Member States.**

Some most relevant provisions of that Directive to understand its essence:

Article 1(1)	This Directive lays down the rules relating to the protection of natural persons with regard to the **processing** of personal data **by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.**
Article 4	**Principles** relating to processing of personal data: (1) Member States shall provide for personal data to be: a) processed **lawfully and fairly;** b) collected for **specified, explicit and legitimate purposes** and **not processed in a manner that is incompatible with those purposes**; c) **adequate, relevant and not excessive** in relation to the purposes for which they are processed; d) **accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

[40] DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680, accessed 31.10.2019.

	e) **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;** f) processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Article 10	Processing of **special categories of personal data**: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, **biometric data for the purpose of uniquely identifying a natural person**, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be allowed only** where strictly necessary, **subject to appropriate safeguards** for the rights and freedoms of the data subject, **and only:** a) where authorised by Union or Member State law; b) to protect the vital interests of the data subject or of another natural person; **or** c) where such processing relates to data which are manifestly made public by the data subject.

The EU adopted legal instruments in the field of judicial cooperation in criminal matters before adopting Directive (EU) 2016/680. Article 61 of the Directive states that these specific provisions of acts should remain unaffected. In addition, the Directive states in its Recitals that the European Commission should evaluate the relationship between Directive (EU) 2016/680 and those acts previously adopted. Article 62 states that the Commission should evaluate the need to adjust and, if necessary, make proposals to create coherent legal rules for those provisions with Directive (EU) 2016/680. This is to ensure that the protection of personal data is guaranteed equally everywhere in the EU. According to Article 63 (5), all Member States must communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

2. Other specific legal instruments in the EU:

2.1. PRÜM Convention[41]

This Convention is ratified by at least 14 Member States: Austria, Belgium, Bulgaria, Estonia, Finland, France, Germany, Hungary, Luxembourg, Netherlands, Romania, Slovakia, Slovenia, Spain. **This Convention does not regulate the exchange of facial images.**

Some of the most relevant provisions of the Convention to understand its essence:

Article 1(1)	By means of this Convention, the Contracting Parties **intend to step up cross-border cooperation, particularly mutual exchange of information.**
Article 10	Supply of further personal data and other information - should the procedure referred to in Article 9 show **a match between fingerprinting data**, the supply of any available further personal data and other information relating to the reference data **shall be governed by the national law, including the legal assistance rules, of the requested Contracting Party.**
Article 14	(1) For the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings, the Contracting Parties shall, both upon request and of their own accord, **in compliance with the supplying Contracting Party's national law**, supply one another with personal data if any final convictions or other circumstances give reason to believe that the data subjects will commit criminal offences at the event or pose a threat to public order and security, in so far as the supply of such data is permitted under the supplying Contracting Party's national law. (2) **Personal data may be processed only** for the purposes laid down in paragraph 1 and for the specified event for which they were supplied. **The data supplied must be deleted without delay once the**

[41] Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed by the contracting parties in Prüm (Germany) on 27 May 2005. Online available: https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/prumtr.pdf, accessed 31.10.2019.

	purposes referred to in paragraph 1 have been achieved or are no longer achievable. The data supplied must in any event be deleted after not more than a year.

2.2. Council Decision 2008/615/JHA[42]

This Decision has been replaced by Directive (EU) 2016/680 by now[43], but it was an important legal instrument for 10 years, giving guidance in cross-border cooperation between Member States:

Article 26	(1) Processing of personal data by the receiving Member State shall be permitted **solely for the purposes for which the data have been supplied in accordance with this Decision.** Processing for other purposes shall be permitted solely with the **prior authorisation of the Member State administering the file and subject only to the national law of the receiving Member State.** Such authorisation may be granted provided that processing for such other purposes is permitted under the national law of the Member State administering the file. (2): Processing of data supplied pursuant to Articles 3, 4 and 9 by the searching or comparing Member State shall be permitted solely in order to: a) establish whether the compared DNA profiles or **dactyloscopic data** match; b) prepare and submit a **police or judicial request** for legal assistance in compliance with national law **if those data match;** c) record within the meaning of Article 30. The Member State administering the file may process the data supplied to it in accordance with Articles 3, 4 and 9 **solely where this**

[42] DECISION OF THE EUROPEAN UNION 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615, accessed 31.10.2019.

[43] Article 59 of the Directive 2016/690. EDPB website about legal framework: https://edpb.europa.eu/legal-framework_en

	is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to Article 30. **The supplied data shall be deleted immediately** following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under points (b) and (c) of the first subparagraph.

2.3. Eurodac Regulation[44]

Recital 8	It is essential in the fight against terrorist offences and other erious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation of terrorist offences as referred to in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. Therefore, the data in Eurodac should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of Member States and the European Police Office (Europol).

[44] REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast). Online available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:EN:PDF, accessed 31.10.2019.

Recital 13	Since Eurodac was originally established to facilitate the application of the Dublin Convention, access to Eurodac for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes a change of the original purpose of Eurodac, which interferes with the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to protect a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.
Recital 31	For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of Eurodac data should only take place in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist offence or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that they will commit or have committed any such offence. A specific case also exists when the request for comparison is connected to a person who is the victim of a terrorist offence or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with Eurodac when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence.
Recital 33	Prior to searching Eurodac, designated authorities should also, provided that the conditions for a comparison are met, consult the

	Visa Information System under Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

2.4. VIS Regulation[45]

Article 3	Availability of data for the prevention, detection and investigation of terrorist offences and other serious criminal offences. 1. The designated authorities of the Member States may in a specific case and following a reasoned written or electronic request access the data kept in the VIS referred to in Articles 9 to 14 if there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences. Europol may access the VIS within the limits of its mandate and when necessary for the performance of its tasks. 2. The consultation referred to in paragraph 1 shall be carried out through central access point(s) which shall be responsible for ensuring strict compliance with the conditions for access and the procedures established in Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by the designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Member States may designate more than one central access point to reflect their organisational and administrative structure in fulfilment of their constitutional or legal requirements. In an exceptional case of urgency, the central access point(s) may receive written, electronic or oral requests and only verify *ex-post*

[45] REGULATION (EC) No 767/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). Online available: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32008R0767, accessed 31.10.2019.

	whether all the conditions for access are fulfilled, including whether an exceptional case of urgency existed. The *ex-post* verification shall take place without undue delay after the processing of the request. 3. Data obtained from the VIS pursuant to the Decision referred to in paragraph 2 shall not be transferred or made available to a third country or to an international organisation. However, in an exceptional case of urgency, such data may be transferred or made available to a third country or an international organisation exclusively for the purposes of the prevention and detection of terrorist offences and of other serious criminal offences and under the conditions set out in that Decision. In accordance with national law, Member States shall ensure that records on such transfers are kept and make them available to national data protection authorities on request. The transfer of data by the Member State which entered the data in the VIS shall be subject to the national law of that Member State. 4. This Regulation is without prejudice to any obligations under applicable national law for the communication of information on any criminal activity detected by the authorities referred to in Article 6 in the course of their duties to the responsible authorities for the purposes of preventing, investigating and prosecuting the related criminal offences.

2.5. Schengen II Decision[46]

Recital 5	SIS II should constitute a compensatory measure contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between police authorities and judicial authorities in criminal matters.
Article 22	**Specific rules for photographs and fingerprints**

[46] COUNCIL DECISION 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Online available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0533, accessed 31.10.2019.

	The **use of photographs** and fingerprints as referred to in Article 20(3)(e) and (f) shall be used subject to the following provisions: (a) photographs and fingerprints shall only be entered following a special quality check to ascertain the fulfilment of a minimum data quality standard. The specification of the special quality check shall be established in accordance with the procedure referred to in Article 67, without prejudice to the provisions of the instrument setting up the Management Authority; (b) photographs and fingerprints shall only be used to confirm the identity of a person who has been located as a result of an alphanumeric search made in SIS II.
Article 40	**1.** Access to data entered in SIS II and the right to search such data directly or in a copy of SIS II data shall be reserved exclusively to the authorities responsible for: (b) other police and customs checks carried out within the Member State concerned, the coordination of such checks by designated authorities.
Article 41	1. The European Police Office (Europol) shall within its mandate have the right to access and search directly, data entered into SIS II in accordance with Articles 26, 36 and 38.

2.6. Europol Regulation[47]

Recital 25	Europol should ensure that all personal data processed for operational analyses are allocated a specific purpose. Nonetheless, in order for Europol to fulfil its mission, it should be allowed to process all personal data received to identify links between multiple crime areas and investigations and should not be limited to identifying connections only within one crime area.
Recital 33	All Member States are affiliated to Interpol. To fulfil its mission, Interpol receives, stores and circulates data to assist competent law

[47] REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794, accessed 31.10.2019.

	enforcement authorities to prevent and combat international crime. Therefore, it is appropriate to strengthen cooperation between Europol and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. When personal data is transferred from Europol to Interpol, this Regulation, in particular the provisions on international transfers, should apply.
Article 2	**(h) 'personal data' means any information relating to a data subject;** (k) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (m) 'transfer of personal data' means the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data;
Article 18	2. Personal data may be processed only for the purposes of: (a) cross-checking aimed at identifying connections or other relevant links between information related to: (i) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence; (ii) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent; (b) analyses of a strategic or thematic nature; (c) operational analyses;

	(d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations.

2.7. Eurojust Decision[48]

Recital 14	Eurojust should be authorised to process certain personal data on persons who, under the national legislation of the Member States concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Eurojust is competent, or who have been convicted of such an offence. The list of such personal data should include telephone numbers, e-mail addresses, vehicle registration data, DNA profiles established from the non-coding part of DNA, photographs and fingerprints. The list should also include traffic data and location data and the related data necessary to identify the subscriber or user of a publicly available electronic communications service; this should not include data revealing the content of the communication. It is not intended that Eurojust carry out an automated comparison of DNA profiles or fingerprints.
Article 15	1. When processing data in accordance with Article 14(1), Eurojust may process only the following personal data on persons who, under the national legislation of the Member States concerned are suspected of having committed or having taken part in a criminal offence in respect of which Eurojust is competent or who have been convicted of such an offence: (n) DNA profiles established from the non-coding part of DNA, photographs and fingerprints.

[48] COUNCIL DECISION 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. Online available: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Consolidated%20version%20of%20the%20Eurojust%20Council%20Decision/Eurojust-Council-Decision-2009Consolidated-EN.pdf, accessed 31.10.2019.

2.8. Council Framework Decision[49]

Article 8	2. The use of information and intelligence which has been exchanged directly or bilaterally under this Framework Decision shall be subject to the national data protection provisions of the receiving Member State, where the information and intelligence shall be subject to the same data protection rules as if they had been gathered in the receiving Member State. The personal data processed in the context of the implementation of this Framework Decision shall be protected in accordance with the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and, for those Member States which have ratified it, the Additional Protocol of 8 November 2001 to that Convention, regarding Supervisory Authorities and Transborder Data Flows. The principles of Recommendation No. R(87) 15 of the Council of Europe Regulating the Use of Personal Data in the Police Sector should also be taken into account when law enforcement authorities handle personal data obtained under this Framework Decision.

In brief summation, adopted in April 2016, the new EU data protection framework comprises:

1) a General Data Protection Regulation (Regulation 2016/679 or GDPR), which replaced the Data Protection Directive;

2) a Directive on the protection of personal data processed for law enforcement purposes (Directive (EU) 2016/680), which replaced Council Framework Decision 2008/977/JHA.

EU legal instrument on data protection	Definition of 'biometric data' (including 'facial image')	Personal scope	Material scope
Law Enforcement Directive (Directive EU 2016/680)	Yes, Article 3 (13)	EU Member States' law enforcement authorities	Automated processing of personal data in Schengen Member States and processing of

[49] COUNCIL FRAMEWORK DECISION 2006/960/JH of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960, accessed 31.10.2019.

			personal data by any means which form part of a filing system for the prevention, investigation, detection or prosecution of criminal offences – within the scope of EU law
GDPR (Regulation EU 2016/679)	**Yes, Article 4 (14)**	**All private actors established and public institutions operating in the EU as well as controllers and processors not established in the EU that offer goods and services to data subjects in the EU**	**Automated processing of personal data in the European Economic Area and processing of personal data by any other means which form part of a filing system – within the scope of EU law (e.g. GDPR not applicable to national security-related data processing)**

Source: FRA, European Union Agency for Fundamental Rights, 2019 Table 1: EU law instruments on data protection: provisions on facial images and their applicability[50]

The following key points are relevant in EU law on data protection in police and criminal justice matters:[51]

1) Within the EU, data protection in the police and criminal justice sector is regulated in the context of both national and cross-border processing by police and criminal justice **authorities of Member States and EU actors.**

2) At the Member State level, Directive (EU) 2016/680 **needed to be incorporated into national law** by 6 May 2018 at the latest.

3) **Specific legal instruments govern data protection in police and law enforcement cross-border cooperation,** particularly in combating terrorism and cross-border crime.

4) Special data protection rules exist for the European Police Office (Europol), the EU Judicial cooperation unit (Eurojust) and the newly established European Public Prosecutor's Office, which are all EU bodies assisting and promoting cross-border law enforcement.

[50] FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019. Online available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf?fbclid=IwAR3ce-bfDFf7mgXia9mSHbNUQFKjbi0Bzs0LMwL82puScHtGWJPINX2PT3U, accessed 28.11.2019.
[51] Handbook on European data protection law. Op.cit.

5) Special data protection rules also exist for the joint information systems that have been established at the EU level for cross-border information exchanges between the competent police and judicial authorities. Important examples are the Schengen Information System II (SIS II), the Visa Information System (VIS) and Eurodac, a centralised system containing the fingerprint data of third-country nationals and stateless persons applying for asylum in one of the EU Member States.

6) **The EU is still in the process of updating the data protection provisions set out above, so as to be in line with the provisions of Directive (EU) 2016/680.** The latter most likely means that the laws of Member States in particular areas are not yet in line with EU legal framework for data protection.

2.2 Legal instruments of the Council of Europe

1. Convention 108+[52]

The Convention **is not directly applicable** and **it obliges Parties to incorporate its provisions into their law** and secure their effective application in practice; how this is done depends on the applicable legal system and the approach taken regarding the incorporation of international treaties.[53]

The Convention was signed by Austria, Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Ireland, Latvia, Lithuania, Luxembourg, Monaco, Netherlands, Norway, Portugal, Spain, Sweden, the UK and 6 (six) non-European states (Uruguay, Cape Verde, Mauritius, Mexico, Senegal and Tunisia).[54]

The most relevant agreements to take into account are the following:

Article 3	Scope 1. Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.
Article 5	Legitimacy of data processing and quality of data

[52] Convention for the protection of individuals with regard to the processing of personal data. Online available: http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (31.10.2019)

[53] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223 Strasbourg, 10.X.2018. Online available: https://rm.coe.int/16808ac91a (12.11.2019)

[54] J. Baker. "What does the newly signed 'Convention 108+' mean for UK adequacy?", 30 October 2018. Online available: https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/ (12.11.2019)

	1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.
Article 6	Special categories of data 1. The processing of: – genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures; – **biometric data uniquely identifying a person;** – personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.
Article 14	Transborder flows of personal data 1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a nonParty, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation. 2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured. 3. An appropriate level of protection can be secured by: a. the law of that State or international organisation, including the applicable international treaties or agreements;

	b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing. 4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if: a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; b. the specific interests of the data subject require it in the particular case; c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression. 5. Each Party shall provide that the competent supervisory authority within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c. 6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

3. Police Recommendation[55] and Practical guide on the use of personal data in the police sector[56]

[55] COUNCIL OF EUROPE COMMITTEE OF MINISTERS RECOMMENDATION No. R (87) 15 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR, 17 September 1987. Online available: https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_87_15.pdf, accessed 30.10.2019.

[56] Practical guide on the use of personal data in the police sector, Strasbourg, 15 February 2018 T-PD(2018)01 Council of Europe. Online available: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5, accessed 30.10.2019.

As data processing by police authorities may have a significant impact on the persons concerned, detailed data protection rules for the processing of personal data in this area are especially necessary. The CoE Police Recommendation sought to address this issue by giving guidance on:

1) how personal data should be collected for police work;
2) how data files in this area should be kept;
3) who should be allowed to access these files, including the conditions for transferring personal data to foreign police authorities;
4) how data subjects should be able to exercise their data protection rights; and
5) how control by independent authorities should be implemented. The obligation to provide adequate data security was also considered.[57]

The recommendation does not provide for the open-ended, indiscriminate collection of personal data by police authorities. It limits the collection of personal data by police authorities to that which is necessary for the prevention of a real danger or the prosecution of a specific criminal offence. Any additional data collection would have to be based on the specific national legislation of the Member State. Processing of sensitive data should be limited to that which is absolutely necessary in the context of a particular inquiry.[58]

4. Cybercrime Convention[59]

While the convention **is not** an instrument aimed at promoting data protection, it **criminalises activities likely to violate a data subject's right to the protection of their data.** Furthermore, it requires Contracting Parties to adopt legislative measures to enable their national authorities to intercept traffic and content data.[60]

Key points to summarise and for consideration:[61]

[57] Handbook on European data protection law. Op.cit.
[58] Handbook on European data protection law. Op.cit.
[59] Convention on Cybercrime, Budapest, 23 November 2001 (European Treaty Series - No. 185) Online available: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561, accessed 31.10.2019.
[60] Handbook on European data protection law. Op.cit.
[61] Handbook on European data protection law. Op.cit.

1) The Modernised Convention 108 and the CoE Police Recommendation apply to data protection across **all areas of police work.**
2) The Cybercrime Convention (Budapest Convention) is a binding **international legal instrument** dealing with crimes committed against and by means of electronic networks. It is also relevant for the investigation of non-cyber-crimes that involve electronic evidence.

One important distinction between Council of Europe and EU law is that CoE law, unlike EU law, applies to the national security area. This means that Contracting Parties need to stay within the remit of Article 8 of the European Convention on Human Rights,[62] even for activities related to national security.[63]

3. NATIONAL LAWS OF ALL EU MEMBER STATES

Both, the General Data Protection Regulation 2016/679 (GDPR) and Law Enforcement Directive (EU) 2016/680 require a legal basis for processing biometric data (including facial images) as sensitive personal data. The legal basis for processing biometric data, including facial images, where the processing is necessary for reasons of substantial public interest, must be stipulated in European Union and/or in Member State law (specific law), which should be preceded by an assessment carried out by the legislator to conclude whether the processing of this sensitive personal data meets the following criteria:

1) is proportionate to the aim pursued
2) respects the essence of the rights to private data protection
3) provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

However, as we stated earlier in this Report, according to Recital[64] 19 of the GDPR, the GDPR is not be applied to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

[62] **Article 8 stipulates the right to respect for private and family life: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.** Online available: https://www.echr.coe.int/Documents/Convention_ENG.pdf, accessed 30.10.2019.

[63] Handbook on European data protection law. Op.cit.

[64] Note: One could regret that the applicability of the Law Enforcement Directive is only mentioned in a **non-binding provision.**

including safeguarding against and the prevention of threats to public security. The free movement and processing of such data is regulated by Directive (EU) 2016/680 of the European Parliament and the Council. **Law enforcement access to and use of personal data should therefore fall into the category of data 'processing', as set out in Article 3 (2) of Directive (EU) 2016/680. So-called cross-use of personal data will be discussed in detail in Chapter 4 of the current legal analysis.**

According to Article 4 (1) of Directive (EU) 2016/680 all Member States must provide for personal data to be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

In the following sections of this Chapter we will analyse laws of all Member States based on 9 (nine) research questions given to us for this public procurement.

3.1. Austria

The following laws regarding offence proceedings, regulate the collection and use of facial images in Austria:

1) Code of Criminal Procedure (Gesamte Rechtsvorschrift für Strafprozessordnung 1975) [65];

2) Immigration Police Act (Gesamte Rechtsvorschrift für Fremdenpolizeigesetz 2005)[66];

3) Administrative Penal Act (Gesamte Rechtsvorschrift für Verwaltungsstrafgesetz 1991)[67];

4) Security Police Act (Bundesgesetz über die Organisation Der Sicherheitsverwaltung und die Ausübung der Sicherheitspolitzei, shortly Sicherheitspolizeigesetz)[68].

The Article 74 (1) of Code of Criminal Procedure gives the general authorization to the criminal police, public prosecutor and court to process the personal data required as part of their duties. Unless otherwise specified for the processing of personal data, the provisions of the Data Protection Act[69] apply. The Article 74 (2) in Code of Criminal Procedure states that the principle of law and proportionality are to follow when processing the personal data. According to Article 118 (2) of Code of Criminal Procedure the criminal police are authorized photograph the person and take their papillary line impressions as necessary to determine their identity. Following Article 118 (1) the identity determination is permitted if, based on certain facts, it can be assumed that a person is involved in a crime, can provide information about the circumstances of the inspection or has left traces that could serve to clarify the situation. Personal data obtained solely on the basis of an identity check (Article 118) may be processed according to Article 75 (4) of Code of Criminal Procedure only as long as the type of the deed, the personality of the person concerned or due to other circumstances is to be feared that this person will commit a criminal offense with no easier consequences. If the accused is legally acquitted or the investigation is discontinued without reserve for subsequent prosecution, this personal data must be deleted.

According to the Article 97 (1) of Code of Criminal Procedure, it is permissible to make an image recording of an interrogation, provided that it is recorded in full, after expressly informing the interrogated person.

The Article 98 (1) of Immigration Police Act authorizes the state police directorates and Austrian representative authorities to process personal data if this is necessary to perform the tasks assigned to them. The state police directorates and Austrian representative authorities may only process personal

---

[65] Gesamte Rechtsvorschrift für Strafprozessordnung 1975, online available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326, accessed 31.10.2019.

[66] Gesamte Rechtsvorschrift für Fremdenpolizeigesetz 2005, online available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004241, accessed 31.10.2019.

[67] Gesamte Rechtsvorschrift für Verwaltungsstrafgesetz 1991, online available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005770, accessed 31.10.2019.

[68] Bundesgesetz über die Organisation Der Sicherheitsverwaltung und die Ausübung der Sicherheitspolitzei 1997, available online: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792.

[69] Bundesgesetz über den Schutz personenbezogener Daten 1999, available online: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.

data of third parties considering Article 98 (2) if their selectability from the total amount of stored data is not provided. This does not apply insofar as it is necessary to determine the total number of data records relating to this third person. The situations where the state police directorates are allow to treat the foreigners for the purpose of establishing his identity are listed in Article 99 (1) of Immigration Police Act. The photo ID is one of the possible documents for foreigners according to the Immigration Police Act. The photos are the identification data in the sense of Article 2 (5) 4) of Immigration Police Act. The photo is required also for the special card in case the stay of strangers in the federal territory is tolerated considering Article 46a of the same act. The card serves to prove the identity of the stranger in the procedure before the Federal Office. The Article 46a (5) states that the card is to withdrawn in the case the photo on the card no longer makes the holder clearly recognizable.

Following Article 34b of Administrative Penal Act the organs of the public security service are authorized to ascertain the identity of a person if he or she is entered in the act or immediately thereafter either credibly accused of committing the act or is entered with objects that indicate that he or she was involved in the act. Article 35 (2) and (3) of the Security Police Act are to be applied accordingly.

Imprisonment Act (Gesamte Rechtsvorschrift für Strafvollzugsgesetz)[70] regulates the collection and use of facial images of detained persons. The Article 132 (4) of Imprisonment Act rules that when the photo is taken or if this is otherwise necessary for purposes of identification, from prisoners may also take photos (and fingerprints) against their will. The security authorities have right to treat prisoners in accordance with the provisions of the Security Police Act.

List of laws regulating issuance and use of identity documents, which regulate the collection and use of facial images in Austria, are:

1) Identity Documents Act (Gesamte Rechtsvorschrift für Passgesetz 1992)[71];

2) University Act (Gesamte Rechtsvorschrift für Universitätsgesetz 2002)[72];

3) Settlement and Residence Act (Gesamte Rechtsvorschrift für Niederlassungs- und Aufenthaltsgesetz)[73];

4) Driving License Act (Gesamte Rechtsvorschrift für Führerscheingesetz)[74].

[70] Gesamte Rechtsvorschrift für Strafvollzugsgesetz 1969, online available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002135, accessed 31.10.2019.

[71] Gesamte Rechtsvorschrift für Passgesetz 1992, online available: https://tinyurl.com/y4gwcfh5, accessed 31.10.2019.

[72] Gesamte Rechtsvorschrift für Universitätsgesetz 2002, online available: https://tinyurl.com/kmrre8x, accessed 31.10.2019.

[73] Gesamte Rechtsvorschrift für Niederlassungs- und Aufenthaltsgesetz 2005, online available: https://tinyurl.com/y3shnun9, accessed 31.10.2019.

[74] Gesamte Rechtsvorschrift für Führerscheingesetz 1997, online available: https://tinyurl.com/yyzpzyv7, accessed 31.10.2019.

Security Police Act regulates the use of data about natural persons, including facial images, by state in case of particular security-related key actions, searches or regulatory events as well as for the fulfillment of the first general obligation to provide assistance.[75]

Article 53 of Security Police Act states that the security authorities may process personal data: a) for the fulfillment of the first general obligation to provide assistance[76], b) for the defense against criminal connections[77], c) for the defense against dangerous attacks[78], including the hazard research necessary in the context of hazard prevention[79], d) for the prevention of probable dangerous attacks against life, health, morality, freedom, property or the environment[80] or for the prevention of dangerous attacks by means of crime analysis, if the type of the attack is likely to be repeated, e) for purposes of the search[81], to maintain public order in a particular event. Article 53 (2) of the Security Police Act gives to the security authorities right to process data that they have processed in compliance with federal or state laws for the purposes and under the conditions set out previously. However, an automated data comparison within the meaning of Article 141 of Code of Criminal Procedure is prohibited. Existing bans on transmission remain unaffected.

The Article 141 of Code of Criminal Procedure regulates the data comparison. The Article 141 (1) states that for the purposes of this Act, "data comparison" is the automated comparison of data (Article 36 (2) No. 1 DSG) of data processing that contains certain features that identify or exclude the suspected perpetrator with data of another data processing that contains such features included to identify individuals who are considered suspects based on these characteristics. The Article 141 (2) states that data comparison is permitted if the investigation of a crime[82] would otherwise be considerably more difficult and only such data is included that the courts, public prosecutors and security authorities use for the purposes of a pending criminal procedure or otherwise on the basis of existing federal or have determined or processed state laws. According to Article 141 (3) in the case the investigation of a crime threatened with more than ten years' imprisonment or a crime pursuant to Article 278a or 278b of the Criminal Code would otherwise be hopeless or significantly more difficult, it is permissible to include data, the courts and prosecutors and the criminal police in a data comparison Article 76 (2) must be transmitted, and data relating to persons who have obtained certain goods or services from a certain company or who are members of private law associations or legal entities under private law or public law must be included.

[75] Article 53a of Security Police Act
[76] Article 19 of Security Police Act
[77] Article 16 Abs. 1 Z 2 and 21 of Security Police Act
[78] Article 16 (2) and (3) and § 21 (2) of Security Police Act
[79] Article 16 (4) and 28a of Security Police Act
[80] Article 22 (2) and (3) of Security Police Act
[81] Article 24 of Security Police Act
[82] Article 17 (1) of Criminal Code

The Article 141 (4) stipulates that special categories of personal data (Article 39 DSG) may not be included in a data comparison. This does not apply to data on citizenship, data relating to the designation of a group of perpetrators as well as data that prosecutors or security authorities have lawfully determined by means of identification measures, by searching a person, by physical examination or by molecular genetic analysis, until this data is only used for a data comparison according to paragraph 2 can be used. Data from associations of persons whose purpose is directly related to one of the specially protected characteristics may not be included in a data comparison under any circumstances.

The facial images are collected from different groups of natural persons:

1) accused, prisoner (according to Criminal Procedure Act, Imprisonment Act, Security Police Act);
2) drivers (according to Driving License Act);
3) persons with identification documents (according to Identity Documents Act);
4) students (according to University Act);
5) foreigners (according to Settlement and Residence Act).

The purposes to use facial images depend on legal basis as follows:

1) In order to grant the identity document (based on Article 22a (3) and 22b (2) of Identity Documents Act), for documentary purposes (based on Imprisonment Act),
2) In order to perform procedures (based on Code of Criminal Procedure),
3) In order to grant the license and to perform procedures (based on Article 16a Driving License Act),
4) In order to grant the identity document (based on Article 35 of Settlement and Residence Act),
5) In order to grant the identity document (based on Article 60 of University Act),
6) In order to grant the identity document (based on Immigration Police Act), for documentary purposes (based on Administrative Penal Act).

There is no information in the abovementioned list of laws regarding the exact database, where the facial images are collected, stored and processed. In some cases, the relevant laws state that the responsible authority has to store the data, but it does not state to where exactly. For instance, the entire legal provision for BFA[83] procedural law (Gesamte Rechtsvorschrift für BFA-Verfahrensgesetz)[84] stipulates that photographs may be processed as part of the Central Aliens Register.

In the Driving License Act are provisions about processing data in the Driving license register[85].

[83] BFA – procedure before the Federal Office for Foreign Affairs and Asylum (Bestimmungen über das Verfahren vor dem Bundesamt für Fremdenwesen und Asyl)

[84] Gesamte Rechtsvorschrift für BFA-Verfahrensgesetz, 2012, online available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007944

[85] § 16a, 16b of Driving License Act

In individual exceptional cases, the security authorities are entitled to process for the specified purposes personal image, which legal entities in the public or private sector have legally processed, using image recording devices and have voluntarily transmitted to the security authority. Processing of personal image data about non-public behavior is not permitted.[86] The Article 57 of Security Police Act lists the situations of central information collection, admissibility of the determination, processing and transmission of data, including photo of a person. Article 57 (3) authorizes the security authorities to process the data they have stored in the central information collection. The queries and transmissions of the data processed in accordance with Article 1, 2 and 2a are permitted to authorities for purposes of security administration, asylum and foreign affairs as well as the administration of criminal justice.

The cross-border cooperation between the countries (between government entities) has to take into consideration the provisions of the Data Protection Act (Datenschutzgesetz), namely Sections 58 and 59 in this Act and Police Cooperation Act (Gesamte Rechtsvorschrift für Polizeikooperationsgesetz)[87].

Data Protection Act has been significantly changed by the Data Protection Adaptation Act 2018, Federal Law Gazette I No. 120/2017. The title is no longer "Data Protection Act 2000" (DSG 2000), but only "Data Protection Act" (Datenschutzgesetz - DSG). The changes are so extensive that almost all references to provisions of the DSG 2000 are no longer valid. Processing of personal data for the purposes of the security police state protection, military self-protection, the investigation and prosecution of criminal offences, the execution of sentences and the execution of measures is stipulated in Article 36-61 of Data Protection Act.[88] It appears that Austrian legislator has chosen to transpose Directive 2016/680 into DSG to the fullest extent by almost mimicking it.

3.2. Belgium

The right to one's own image ('recht op afbeelding' l'droit á l'image) exists in Belgium where it has been created by case law. The right protects one's image as well as, according to some, one's behaviour. The right is based on a so-called 'personality' right to one's image. A personality right has specific characteristics, such that it is universal, absolute, not within someone's property, not fit for transfer or

[86] § 53 of Security Police Act

[87] **Polizeikooperationsgesetz 1997, available online:**
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006019

[88] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DGS), available online https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

expiration and inalienable at death.[89] **There is no specific single legal provision which creates this right under Belgian law**, since the right has been developed by case law under several legal provisions, including without limitation Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 22 of the Belgian Constitution, the Data Protection Act as modified as well as more specific provisions, which refer to the use of images, including but not limited to the Copyright Act.[90] **However, there are limitations to the right to one's image and these limitations should be adopted by specific legislation**.[91]

The following laws regarding offence proceedings regulate the collection and use of facial images in Belgium:

1) Police officer law (Wet op het politieambt) [92]. According to Article 44/11 (1) the technical databases created as a result of the use of intelligent cameras for automatic license plate recognition or of intelligent systems for automatic license plate recognition contain the following data, if they appear on the images of the cameras - if applicable, **a photo of the driver and of the passengers**. (2) This personal data may be stored for a period of no more than twelve months from their registration;

2) Code of Penalty Claim (Wetboek van strafvordering)[93];

3) Basic law concerning the prison system and the legal position of prisoners (Basiswet betreffende het gevangeniswezen en de rechtspositie van de gedetineerden)[94].

For the purpose of identification, Article 107 of the Basic law concerning the prison system and the legal position of prisoners states that the detainee is obliged to prove their identification. The prisoner must give a facial image.

The laws regulating issuance and use of identity documents, which regulate the collection and use of facial images, are the following:

---

[89] E.J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis, p 193.
[90] E.J. Kindt. Op cit., p 194.
[91] E.J. Kindt. Op cit., p 195.
[92] Wet op het politieambt, published 22.12.1992. Online available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1992080552&table_name=wet, accessed 31/10/2019.
[93] Wetboek van strafvordering, published 27.11.1808. Online available: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1808111730&table_name=wet, accessed 31/10/2019.
[94] Basiswet betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, published 01.02.2005. Online available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2005011239, accessed 31/10/2019.

1) Royal Decree concerning identity cards (Koninklijk besluit betreffende de identiteitskaarten)[95]
2) Royal Decree concerning driving licenses (Koninklijk besluit betreffende het rijbewijs)[96]

The groups of people from whom facial images are collected are, in general, citizens (ID Card), holders of driving licenses, suspects, accused, prisoners, detained persons. The purposes that allow the use of facial images are identification, security checks, administration and investigations.

According to the Act containing various provisions regarding the National Register and the population registers, (Wet houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters)[97] the main database in which the facial images are stored is the National Register of Natural Persons. Data Privacy regulations apply in general. According to Article 44/2 § 1 of the Police Officer Act, we can find the following categories of operational police databases that are involved with storing the information (including personal data): The General National Database, the basic databases, the special databases.

The abovementioned Police officer law allows the use of data, including facial images, which have been collected for other (civil) purposes to be used in offence proceedings. The rule is also applicable in the cross-border use of facial images.

It should be also noted that Dr Kindt has given in her comparative legal research a very comprehensive overview of the legal framework for the processing of biometric data in Belgium, referring to the Belgian Commission for the Protection of Privacy (in short CBPL or Belgian DPA) with its critical evaluations and recommendations.[98] One can assume that national law-making is in progress.

[95] Koninklijk besluit betreffende de identiteitskaarten, published 28.03.2003. Online available: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2003032531&table_name=wet, accessed 31.10.2019.
[96] Koninklijk besluit betreffende het rijbewijs, published 30/04/1998. Online available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1998032331&table_name=wet, accessed 31/10/2019.
[97] Wet houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters, published 13.12.2018. Online available: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018112505&table_name=wet, accessed 31.10.2019.
[98] Please see Chapter 5.5.1 Belgium in E.J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis, pages 500 – 516.

Under Belgian data protection legislation, access to personal data held by private parties is, in general, not clearly regulated.[99] There have been court cases in the Supreme Court on the use of camera surveillance and transfer of the images to the police or law enforcement authorities.[100]

3.3. Bulgaria

The following legal acts regarding offence proceedings and detention of the persons, regulate the collection and use of facial images (person's photographs) in Bulgaria:

1) Code of Criminal Procedure (НАКАЗАТЕЛНО-ПРОЦЕСУАЛЕН КОДЕКС)[101].
Article 110 (1) stipulates that the **physical evidence must be** carefully examined, detailed in a relevant protocol and, if possible, **photographed**. Article 125 (1): Where physical evidence cannot be separated from the place where they were found, as well as in other cases provided for in this Code, photographs, slides, films, videos, sound recordings, records on a computer data carrier shall be made, plans, schemes, castings or prints. According to Article 272 (2): In case of doubt about the identity of the defendant, **identification may be made by photographs** or by information of established citizens who know the person;

2) Law on implementation of sentences and detention (ЗАКОН ЗА ИЗПЪЛНЕНИЕ НА НАКАЗАНИЯТА И ЗАДЪРЖАНЕТО ПОД СТРАЖА)[102]. According to Article 48 (2) **Newly incarcerated persons shall be photographed,** and their Bulgarian identity documents seized. If Bulgarian personal documents are not available, the reasons for their absence shall be noted;

3) Rules for the Implementation of Penal Sanctions and Detention in Custody Act (ПРАВИЛНИК ЗА ПРИЛАГАНЕ НА ЗАКОНА ЗА ИЗПЪЛНЕНИЕ НА НАКАЗАНИЯТА И ЗАДЪРЖАНЕТО ПОД СТРАЖА[103]).

[99] Please see discussion a pain points in E.J. Kindt. Op. Cit. p 788.
[100] Please see discussion a pain points in E.J. Kindt. Ibid.
[101] НАКАЗАТЕЛНО-ПРОЦЕСУАЛЕН КОДЕКС, entry into force 29.04.2006. Online available: https://www.lex.bg/bg/laws/ldoc/2135512224, accessed 31.10.2019.
[102] ЗАКОН ЗА ИЗПЪЛНЕНИЕ НА НАКАЗАНИЯТА И ЗАДЪРЖАНЕТО ПОД СТРАЖА, entry into force 01/06/2009. Online available: https://www.lex.bg/laws/ldoc/2135627067, accessed 31.10.2019.
[103] ПРАВИЛНИК ЗА ПРИЛАГАНЕ НА ЗАКОНА ЗА ИЗПЪЛНЕНИЕ НА НАКАЗАНИЯТА И ЗАДЪРЖАНЕТО ПОД СТРАЖА, last modified 10.02.2017. Online available: https://www.lex.bg/laws/ldoc/2135661301, accessed 31.10.2019.

According to Article 28 (7) **Photographing of newcomers (newly arrived prisoners) shall be for the purposes of the execution of the sentence of imprisonment or of the measure of imprisonment**;

4) Ministry of Interior Act (ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ)[104]. According to Article 68 (1) The police authorities shall register the persons who have been prosecuted for a premeditated crime of general nature. The pre-trial authorities are obliged to take the necessary measures to carry out the registration by the police authorities and (3) For the purposes of police registration, **police authorities** shall fingerprint and **photograph the persons**.

Bulgarian Personal Documents Act (ЗАКОН ЗА БЪЛГАРСКИТЕ ЛИЧНИ ДОКУМЕНТИ) [105] regulates issuance and use of identity documents (passport, identity card) regarding the collection and use of facial images.

In addition to the above-mentioned general acts Special Intelligence Means Act (ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА)[106] regulates the collection and use of facial images. According to Article 2 of this Act: (1) the special means of intelligence shall be the technical means and the operational methods for their application, which shall be used to produce physical evidence - film, video, sound recordings, **photographs** and marked objects. (2) technical means are electronic and mechanical equipment, as well as substances that serve to document the activity of controlled persons and objects. (3) operational means shall be the surveillance, tapping, tracing, intrusion marking and interception of correspondence and computerized information, controlled delivery, trusted transaction and investigation through an undercover officer, which are used in the course of applying the technical means under para (2). Article 19b of that Act states that the bodies of the State Agency for Technical Operations carry out activities of surveillance, infiltration, **photographing**, video recording, sound recording, filming, marking of objects and preparation of psychological analysis in connection with the collection of data for protection of the rights and freedoms of citizens, national security and public order.

According to laws regarding offence proceedings in Bulgaria facial images are collected from the following groups of persons:

[104] ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ, last modified 23/07/2019. Online available: https://www.lex.bg/laws/ldoc/2136243824, accessed 31.10.2019.
[105] ЗАКОН ЗА БЪЛГАРСКИТЕ ЛИЧНИ ДОКУМЕНТИ, entry into force 01.04.1999. Online available: https://www.lex.bg/bg/laws/ldoc/2134424576, accessed 31.10.2019.
[106] ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА, last modified 07.05.2019. Online available: https://lex.bg/laws/ldoc/2134163459, accessed 31.10.2019.

1) Accused - in cases of intentional offences prosecuted by public prosecution (based on Ministry of Interior Act);
2) Defendants (based on Code of Criminal Procedure);
3) Prisoners (based on Implementation of Penal Sanctions and Detention in Custody Act);
4) Persons of interest within investigation of grave criminal offences or in relation to national security as well as persons who have consented to the use of special intelligence means for the purpose of protecting their life or property (based on Special Intelligence Means Act);

Facial images of Bulgarian citizens and aliens residing in Bulgaria are collected out of offence proceedings under the Personal Documents Act.

The purposes to use facial images according to the following acts are:
1) Code of Criminal Procedure - verification of identity;
2) Implementation of Penal Sanctions and Detention in Custody Act - to perform prison procedures;
3) Ministry of Interior Act - registration of accused persons; identification;
4) Special Intelligence Means Act - for protection of the rights and freedoms of citizens, national security and public order.

According to the laws the facial images are stored in following databases:
1) Personal dossiers of new entrants to the prison (based on Implementation of Penal Sanctions and Detention in Custody Act);
2) Document informational funds and automated informational funds (based on Ministry of Interior Act).

In principle, above-mentioned laws allow to use photos which have been collected for other (civil) purposes, as material evidence in offence proceedings as long as such photos serve to clarify the circumstances of the case.

Cross-border cooperation in case of exchanging evidences is possible with competent authorities in EU Member States or the Schengen countries with the purpose of preventing, solving and investigating crimes under control of the Bulgarian Ministry of Interior.

3.4. Cyprus

The Cyprus legal system is predominantly based on the English legal system and on the principles of common law and equity.[107] "The legal system which has been in force since the Republic of Cyprus was established retains the influence of the English legal system.

In principle the courts of the Republic of Cyprus apply the following laws:

1) the Constitution of the Republic of Cyprus (*Σύνταγμα της Κυπριακής Δημοκρατίας*);

2) the laws retained by virtue of Article 188 of the Constitution;

3) The principles of common law and the principles of equity;

4) the laws passed by the House of Representatives (*Βουλή των Αντιπροσώπων*).[108]

Currently the Republic is following a process to upgrade and manage Cyprus's system for biometric data collection, centralized personalization, and issuance of electronic passports, ID cards and residence permits.[109] "Upgrading efforts will involve removing outdated hardware and software equipment and replacing it with up-to-date units."[110] Planned for release in the spring of 2020, the modernized documents will feature enhanced security.

The investigation of a crime is carried out by the police, and in exceptional cases the Council of Ministers or the Attorney–General may authorize experts for the investigation.[111] Decisions to prosecute are, as a rule, taken by the police under the overall instructions of the Attorney–General, and in serious criminal cases the decision is taken by the Attorney–General.[112] "As regards the surveillance and maintenance of the security of borders against illegal immigration, the Aliens and Immigration, Port and Marine Police and Air Aviation Police Units with the cooperation of Cyprus Police Academy, are entrusted with the effective control of aliens at entry/exit points, surveillance of the coast and territorial limits of the Republic, provision of relevant training to police officers, prevention of illegal immigration to the territory of the Republic, combating of illegal immigration flow to Cyprus and to other member states of the EU."[113]

---

[107] Judicial systems in Member States – Cyprus, available at https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-cy-en.do?member=1, accessed 31.12.2019.

[108] Judicial systems in Member States. Op.cit.

[109] Luana Pascu, Veridos to upgrade Cyprus biometric passport and data collection system (2019), available at : https://www.biometricupdate.com/201911/veridos-to-upgrade-cyprus-biometric-passport-and-data-collection-system, accessed 31.10.2019.

[110] Ibid.

[111] Rights of defendants in criminal proceedings - Cyprus, available at https://e-justice.europa.eu/content_rights_of_defendants_in_criminal_proceedings_-169-CY-maximizeMS-en.do?clang=en&idSubpage=2&member=1, accessed 31.10.2019.

[112] Ibid.

[113] Frontex, National Authorities, available at: https://frontex.europa.eu/partners/national-authorities/c, accessed 31.10.2019.

The Cypriot intelligence agency (Cypriot Information Service, hereinafter as CIS), is responsible for the protection and promotion of the national and state interests of Cyprus; the prevention and management of activities which constitute a threat against the security and sovereignty of Cyprus and the prevention and combating of activities of terrorist organisations and of organised crime.[114] "The mission must be carried out 'in the framework of respect for fundamental human rights, the Constitution and the laws' and in compliance with the data protection legislation.[115] This means that the intelligence authority can process personal data only in compliance with the data protection law and that the Data Protection Authority (DPA) can exercise over the intelligence authority the oversight foreseen by the data protection legislation, which includes access to records where personal data is maintained except to data revealing the identity of collaborators in records kept for national security purposes or for the purpose of investigating particularly serious crimes. This check is performed by the Commissioner himself or herself or by a DPA officer specifically authorised for this by the Commissioner. Records kept for national security purposes can be checked only in the presence of the Commissioner.[116]"[117] The mandate of the CIS is described in the law includes the search for, collection, evaluation, processing and supply of data, information and Evidence.[118]

The laws in Cyprus in general allow the use of data (under specific conditions), including facial images, which has been collected for other (meaning civil) purposes to be used in offence proceedings, to the collection and use of evidence applicable Criminal Procedure law applies.

Facial images can be collected for example from suspect, accused, prisoner, detained persons in Detention House. "Any party to a proceeding can request the court to order another party to disclose under oath the documents that are or were in his or her possession and relate to the matters of the proceedings, and to allow for their inspection."[119]

---

[114] National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Cyprus (01.07.2016), FRANET contractor: University of Nicosia and Symfiliosi Author(s) name(s): Corina Demetriou, available at: https://fra.europa.eu/sites/default/files/fra_uploads/cyprus-study-data-surveillance-ii-cy.pdf, accessed 20.11.2019.

[115] Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών) N. 75(I)/2016, articles 4 and 5(2), available at www.cylaw.org/nomoi/arith/2016_1_075.pdf

[116] Cyprus, Law on the processing of personal data (Protection of the individual) of 2001 [Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001] N. 138(I)/2001, article 23(h), available at http://cylaw.org/nomoi/enop/non-ind/2001_1_138/full.html

[117] National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Cyprus (01.07.2016), Op.cit.

[118] Ibid.

[119] Litigation and enforcement in Cyprus: overview by Stavros Pavlou, Chrysostomos Nicolaou, Katerina Philippidou and Georgia Siopacha, Patrikios Pavlou & Associates LLC, available at: https://uk.practicallaw.thomsonreuters.com/7-502-0202?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

"In December 2015 the old law of 1996 on confidentiality of private communications, was amended by widening its scope of application.[120] The new law (with further amendments under consideration by Parliament) covers private communications of any form which are recorded or stored in any document, equipment or object and includes content recorded in letters, electronic messages such as SMS, MMS or emails or other internet messages. The law regulating the interception of private communications provides for a procedure in court, which must be initiated by the Attorney General who may act on his own behalf or on behalf of the Chief of the Police or any investigator and not by intelligence agencies.[121]"[122]

Access to the files of the intelligence services (CIS) is permitted only to:
- the CIS director,
- the CIS staff members who are specifically authorised by the director and
- the members of an Advisory Committee set up under the legislation to access the archives of the CIS.[123]"[124]

In regard with processing facial images, attention should be paid to:

- Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018)[125], which was adopted for the effective implementation of certain provisions of the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, and

[120] Cyprus, Law amending the law on protection of confidentiality of private communication (Surveillance of conversations) and access to registered content of private communication of 1996 [Νόμος που τροποποιεί το νόμο περί προστασίας του απορρήτου της ιδιωτικής επικοινωνίας (Παρακολούθηση συνδιαλέξεων) του 1996] N. 216(I)/2015, 31 December 2015, available at http://cylaw.org/nomoi/arith/2015_1_216.pdf

[121] Cyprus, Law amending the law on protection of confidentiality of private communication (Surveillance of conversations) and access to registered content of private communication of 1996 [Νόμος που τροποποιεί το νόμο περί προστασίας του απορρήτου της ιδιωτικής επικοινωνίας (Παρακολούθηση συνδιαλέξεων) του 1996] N. 216(I)/2015, 31 December 2015, available at
http://cylaw.org/nomoi/arith/2015_1_216.pdf

[122] National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Cyprus (01.07.2016), Op.cit.

[123] Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών) N. 75(I)/2016, article 10(1)(b), available at www.cylaw.org/nomoi/arith/2016_1_075.pdf

[124] National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Cyprus (01.07.2016), Op.cit.

[125] Law 125(I)/2018, available at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3b_en/page3b_en?opendocument, accessed 31.10.2019.

- Law on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Law 44(I)/2019).[126]

Laws regulating issuance and use of identity documents (passport, identity card, driving licence), which regulate the collection and use of facial images are Civil Registry Law (Law 141(I)/2002)[127] and Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018)[128].

If, at the discretion of the competent authorities, any details entered in the Register with respect to any person who is recorded or deemed to have been registered under the law are, or have been, inaccurate or misleading after registration, or any photo that is automatically transferred to any identity card is not, or does not have, or may cease to be similar to the citizen, the registration authority may ask the affected person to hand over their identity card and call it submit a new application, as specified, for the issuance of a new identity card to replace the returned card.[129]

Processing of identification data such as facial images can be performed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This would in principle fall within the scope of the work of the Police, Customs Office, Tax authorities, Unit for Combating Money Laundering. The Commissioner for personal data protection is an independent public authority responsible for monitoring the implementation of Regulation (EU) 2016/679 (GDPR) and other laws aiming at the protection of individuals with regards to the processing of their personal data.

Databases of facial images that will be used for facial recognition in offence proceedings: there was no information about specific laws regulating databases, where facial images are stored and processed.

[126] Law 44(I)/2019, available at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/A5C70C14703B857DC225820A004B5CA0/$file/Law%202019_1_044.pdf
[127] Civil Registry Law (Law 141(I)/2002), available at: http://www.cylaw.org/nomoi/enop/non-ind/2002_1_141/full.html, accessed 31.10.2019.
[128] Law 125(I)/2018, Op.cit.
[129] Article 64 of the Civil Registry Law (Law 141(I)/2002), Op.cit.

In 2019 the Justice system initiated a key reform to adopt a web-based Court administration system (eJustice system).[130] "The Civil Registry in Cyprus is under the responsibility of the Interior Ministry, with data gathered locally."[131] "No overarching body nor structure governing or coordinating base registries at an organisational level has been identified in Cyprus."[132] For example in order to receive a Criminal Record Certificate, which is under responsibility of Cyprus Police, physical presence is required because the service is not online.[133]

In 2019 the IT infrastructure for eInvoice in Cyprus was built, while eDelivery in Cyprus was implemented as a pilot to connect municipalities with the Union of Cyprus Municipalities.[134] "The CEF eDelivery building block supports public administrations exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way."[135] Department of Information Technology Services (DITS) is the Government body that coordinates the promotion and application of Information Technology and eGovernment in the public sector and has the mission to plan, develop, implement, manage and maintain the Information and Communication Technology (ICT) systems.[136]

Facial data exchange between EU member states

The laws of Cyprus allow the usage of facial images collected in Cyprus to be used also by other countries (government entities) for the purpose of offence proceedings in these countries. The cross-border cooperation is possible between the countries (government entities) based on Law 2(III) of 2000 on Mutual Assistance in Criminal Matters[137], Law 20 (III) of 2000 ratifying the European convention on criminal procedures,[138] Law 23(I)/2001 on International Co-operation on Criminal Matters,[139]as well as through various international and bilateral agreements (i.e. EU Regulation on co-operation on criminal matters).

---

[130] Digital Government Factsheet 2019 – Cyprus, available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Cyprus_2019_0.pdf, accessed 20.11.2019.
[131] Digital Government Factsheet 2019, Op.cit.
[132] Ibid.
[133] Digital Government Factsheet 2019, Op.cit.
[134] Ibid.
[135] eDelivery in Cyprus, available at: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-cy-ia-0054, accessed 20.11.2019.
[136] Digital Government Factsheet 2019, Op.cit.
[137] Law 2(III) of 2000 on Mutual Assistance in Criminal Matters, available at: http://www.cylaw.org/nomoi/arith/2000_3_002.pdf, accessed 31.10.2019.
[138] Law 20 (III) of 2000 ratifying the European convention on criminal procedures, available at: http://www.cylaw.org/nomoi/arith/2000_3_002.pdf, accessed 31.10.2019.
[139] Law 23(I)/2001 on International Co-operation on Criminal Matters, available at: http://www.cylaw.org/nomoi/indexes/2001_1_23.html, accessed 31.10.2019.

"Under bilateral treaties and multinational conventions that Cyprus has entered into, the courts can assist in the taking of evidence from witnesses or experts on the request of a foreign court.

Cyprus is a signatory to the HCCH Convention on the Taking of Evidence Abroad in Civil and Commercial Matters 1970. As an EU member state, Cyprus is also bound by Regulation (EC) 1206/2001 on co-operation between the courts of the member states in the taking of evidence in civil or commercial matters, which provides for a 90-day deadline for the execution of a request for the taking of evidence, facilitating expeditious assistance among the courts of member states."[140]

3.5. Czech Republic

In some countries, such as Czech Republic, biometric data are mentioned in the general data protection legislation with a list of sensitive data.[141] However, it is not explained whether this is for reasons of identification functionality or otherwise.[142]

The following laws regarding offence proceedings, regulate the collection and use of facial images in Czech Republic:

1) Code of Criminal Procedure[143]

2) Police Act[144] (especially Chapter 4: 'Processing of information by the police')

The Act on the Prison and Justice Guard (*Zákon o výkonu trestu odnětí svobody a o změně některých souvisejících zákonů*)[145] regulates the detention of persons, but there is no information related to the collection and use of facial images.

---

[140] Litigation and enforcement in Cyprus, op.cit.

[141] Reference made in: E.J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis, p 747.

[142] E.J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis, p 783.

[143] Code of Criminal Procedure of the Czech Republic, entry into force 01.01.1962. Online available: https://www.legislationline.org/download/id/6371/file/Czech%20Republic_CPC_1961_am2012_en.pdf, accessed 31.10.2019.

[144] Act of the Czech National Council of 21 June 1991 regulating the Police of the Czech Republic. Online available: https://www.legislationline.org/download/id/1020/file/087ab6b8f317a8515e647ae55747.pdf, accessed 31.10.2019.

[145] Zákon o výkonu trestu odnětí svobody a o změně některých souvisejících zákonů, entry into force 01.01.2000. Online available: https://www.zakonyprolidi.cz/cs/1999-169, accessed 31.10.2019.

Section 89 (2) of the Code of Criminal Procedure stipulates that evidence may be anything that can help to clarify the case, in particular testimonies of the accused and witnesses, expert opinions, items and documents relevant to the criminal proceedings, and examinations. Each party may find, present, or propose to produce evidence. The fact, that the law enforcement authority did not find or request a piece of evidence, is not legal basis for rejecting such evidence. Section 47a(2) of the Police Act stipulates, that the Police may in performing their tasks request the provision of information from databases and registers, allow to use data, **including facial images,** which has been collected for other (civil) purposes in offence proceedings. It is not stipulated whether the latter is possible in cross-border occasions.

Section 42d of the Police Act stipulates that the Police shall process under this Act and special legal regulations 17b) information including personal data collected during the performance of police tasks, to the extent indispensable for the performance of these tasks.

Section 42e (1) of the Police Act states that a police officer who, during the performance of police tasks, cannot obtain personal data that would enable future identification in a different manner is entitled, in the cases of persons accused of a crime or found persons for whom a nation-wide search has been launched and who do not have full legal capacity: (a) to take fingerprints, (b) to detect physical features, (c) to perform antropometrical measurements, (d) to make visual, sound and similar recordings, or (e) to take biological samples in order to obtain information on the genetic equipment.

Special provisions to process personal data are the following. However, it should be noted that namely 'biometric data' or 'facial images' are not mentoned in these provisions although biometric data is considered to be sensitive personal data.

Section 42g (1) stipulates that when preventing and detecting crime, detecting offenders and conducting criminal investigation (hereinafter only "performing police tasks in connection with criminal proceedings"), the Police, while processing personal data, must: (a) determine the purpose for which the personal data are to be processed; (b) collect only such personal data as are relevant for the determined purpose and to the extent indispensable for achieving that purpose; (c) retain the personal data only for the period necessary for the purpose of their processing; (d) process the personal data under this provision separately from personal data processed during the performance of other police tasks; (e) without delay report to the Office for the Protection of Personal Data 17c) the creation of any records containing personal data; this report shall include the name of the department responsible for the processing of the personal data, the purpose of the records, the categories of persons whose data are

processed and of the personal data regarding these persons, and a description of measures for ensuring the required protection of the personal data.

(2) When processing personal data under paragraph (1), the Police are entitled, to the extent necessary for the performance of police tasks in connection with criminal proceedings: (a) to associate personal data which were obtained for different purposes, (b) to process untrue, inaccurate and unverified personal data; these personal data have to be marked as such.

(3) When processing personal data under paragraph (1), the Police are entitled to process sensitive information, 17d) provided it is necessary, with respect to the nature of the crime, for the performance of police tasks in connection with criminal proceedings.

(4) The Police shall process personal data under paragraph (1) also without the persons' consent; at the same time, they must respect the persons' right to the protection of their private and personal life. As soon as it does not jeopardize the accomplishment of police tasks in connection with criminal proceedings, the Police must inform the respective person that they have been processing his/her personal data, or destroy those personal data.

(5) The Police shall not destroy the personal data if these personal data are part of files and have not been processed electronically.

(6) Under the provisions of this Title, the Police shall process personal data also when preventing and detecting criminal offenses the elements of which are listed in the Penal Code 17e) and the perpetrators of which are not criminally liable because of their young age or insanity, and when establishing these offenders.

Section 42h of Police Act regulates processing of personal data during a search for persons. (1) When searching for persons for whom a search has been launched, the Police are entitled: (a) to associate, to the necessary extent, personal data obtained for different purposes, and (b) to process sensitive data of these persons should that be necessary for their finding.

(2) The Police shall destroy the personal data of a missing or wanted person without unreasonable delay after the person has been found. The destruction of the personal data shall not be required if: (a) the person has been missing or wanted repeatedly; (b) there are reasonable grounds to presume that the person will be missing or wanted again; (c) his/her personal data are processed within the performance of police tasks in connection with criminal proceedings.

Section 42i regulates checking the necessity of further processing of personal data

(1) The Police shall at least once in three years check whether the processed personal data are still needed for the performance of police tasks in connection with criminal proceedings or for a search for persons. If the Police find out during that checking or while processing personal data that the data are no longer needed for the performance of police tasks in connection with criminal proceedings or a search for persons, they shall destroy those personal data without unreasonable delay.

(2) For the purposes of the checking under paragraph (1), the investigative, prosecuting and adjudicating bodies, the Ministry of Justice, the Constitutional Court and the Office of the President of the Republic, within the limits of their respective competence, must continuously inform the Police of the final and conclusive decisions of the investigative, prosecuting and adjudicating bodies, the limitations of criminal prosecution, the executions of punishment or the decisions of the President of the Republic regarding criminal proceedings, punishments or granted amnesty.

Section 42j regulates information about personal data and the correction of untrue or inaccurate personal data:

(1) Upon a written request, the Police shall, free of charge, inform the requesting person about the personal data relating to him/her, and shall do so within 30 days of the delivery of that request.

(2) Upon a written request, the Police shall, free of charge, destroy or correct untrue or inaccurate personal data relating to the requesting person, and shall do so immediately upon the delivery of that request.

(3) The requests under paragraphs (1) and (2) shall be decided by the Police Presidium of the Czech Republic; a new request may be submitted no sooner than one year after the submission of the previous request.

(4) The Police shall not grant the request under paragraphs (1) and (2) if this would (a) jeopardize the accomplishment of police tasks in connection with criminal proceedings, or

(b) endanger legitimate interests of a third person;
should the request not be granted, the reasons for the decision on the application must be given in writing.

(5) If the Police are not processing any personal data relating to the requesting person, or the information about the reasoned decision would jeopardize the accomplishment of police tasks in connection with criminal proceedings, the requesting person shall be notified in writing that the Police are processing no personal data relating to the requesting person.

(6) The procedure of handling the request shall not be affected by the Rules of Administrative Procedure.

List of laws regulating issuance and use of identity documents, which regulate the collection and use of facial images in Czech Republic:

1) Act on the Residence of Foreign Nationals in the Czech Republic[146]

2) Act on Identity Cards (*Zákon o občanských průkazech)*[147]

3) Act on Travel Documents (*Zákon o cestovních dokladech)*[148]

4) Traffic Act (*Zákon o provozu na pozemních komunikacích a o změnách některých zákonů)*[149]

Section 18 of the Rules of Administrative Procedure (*Zákon správní řád)*[150] allows a video or audio recording of the oral hearing to be made in interrogation processes in addition to the protocol.

The facial images are collected from different groups of natural persons:

1) suspects
2) accused persons
3) prisoners

The purposes of using facial images depend on a legal basis as follows:

1) to identify the person and perform procedures (based on the Code of Criminal Procedure, Act on Travel Documents)

2) to grant an identity document (based on the Act on Identity Cards)

3) to grant a visa or residency (based on the Act on the Residence of Foreign Nationals)

4) to grant a license and perform procedures (based on the Traffic Act)

---

[146] Act on the Residence of Foreign Nationals in the Czech Republic, entry into force 01/01/2000. Online available: https://www.legislationline.org/download/id/5915/file/Czech_Act_residence_foreigners_1999_2014_en.pdf, accessed 31.10.2019.

[147] Zákon o občanských průkazech, entry into force 01.07.2000. Online available: https://www.zakonyprolidi.cz/cs/1999-328, accessed 31.10.2019.

[148] Zákon o cestovních dokladech, entry into force 01.07.2000. Online available: https://www.zakonyprolidi.cz/cs/1999-329/zneni-20180701, accessed 31.10.2019.

[149] Zákon o provozu na pozemních komunikacích a o změnách některých zákonů, entry into force 01.01.2001. Online available: https://www.zakonyprolidi.cz/cs/2000-361?text=, accessed 31.10.2019.

[150] Zákon správní řád, entry into force 01.01.2006. Online available: https://www.zakonyprolidi.cz/cs/2004-500, accessed 31.10.2019.

5) to perform procedures and for documentary purposes (based on the Police Act, Act on the Prison and Justice Guard).

According to information received from Col. Šárka Havránková (Head of International Police Cooperation Division of Czech Republic) on 7 August 2019, facial images are stored in the following databases:

1) The Identity Cards Register

2) The Register of Travel Documents

3) The Register of Drivers

4) The Central Register of Prisoners

Cross-border cooperation regarding the exchange of evidence is possible between countries (government entities) only at the request of the Public Prosecutor.[151]

3.6. Croatia

The following legal acts regarding offence proceedings regulate the collection and use of facial images in Croatia:

1) Law on the Protection of Natural Persons Regarding the Processing and Exchange of Personal Data for the Purpose of Preventing, Investigating, Detecting or Prosecuting Criminal Offenses or Executing Criminal Sanctions (*Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija*)[152].

This Act lays down the rules of protection of natural persons in relation to the processing and exchange of personal data (including biometrical data) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including protection against threats to public safety and the prevention of such threats;

[151] Filled questionnaire by Col. Šárka Havránková (Head of International Police Cooperation Division of Czech Republic), received on 7th August 2019.

[152] Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, entry into force 04/08/2018. Online available: https://www.zakon.hr/z/1061/Zakon-o-za%C5%A1titi-fizi%C4%8Dkih-osoba-u-vezi-s-obradom-i-razmjenom-osobnih-podataka-, accessed 31.10.2019.

2) Criminal Procedure Code (*Zakon o kaznenom postupku*)[153]. According to Article 211 for the purpose of establishing the identity of a suspect, the police may **photograph**, fingerprint, and enter identity data into appropriate collections. The police may also **publish the suspect's photograph** upon the State Attorney's approval. Article 275 stipulates that the first interrogation of the defendant shall be recorded by an audio- video recording device. Article 301 states that **identification is the determination of the identity of a person**, object, space, sound, mode of movement or other characteristic observed by the defendant or witness, which is established by comparison with another person, object, space, sound, mode of movement or other characteristic and **can also be carried out through appropriate technical devices and programs that allow simultaneous display of photographs or audio-video recordings**;
3) Criminal Code (*Kazneni zakon*)[154];

4) Law on the Police Actions and Authorities (*Zakon o policijskim poslovima i ovlastima*)[155]. According to the Article 49 the **search is announced:** a) for a person suspected of committing a criminal offense for which he or she is prosecuted ex officio or a misdemeanor, or for a person who can give information about the said crime, misdemeanor or perpetrator; b) after the missing person; c) for the person for whom the warrant was issued in accordance with a special law. According to Article 79 (1) in order to prevent offences prosecuted ex officio and misdemeanors, the **police may record public places with audio-video devices** and (2) **if there is a danger** that a public gathering may endanger the life and health of people or property, **the police shall be authorized to carry out audio-video recording and photographing of a public meeting**;

5) Regulations on the Conduct of Police Officers (*Pravilnik o načinu postupanja policijskih službenika*)[156]. According to Article 54 identification of a person is carried out using the methods and means of criminal technique and tactics, and by applying medical and other appropriate procedures, as follows:
a) by checking the data on the civil status of the person (public documents, registers of births, marriages, deaths and other official records),
b) by taking papillary line prints and comparing them with indisputable prints,
c) taking a photo and comparing a photo with an existing one,

[153] Zakon o kaznenom postupku, entry into force 27/07/2017. Online available: https://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku, accessed 31.10.2019.
[154] Kazneni zakon, entry into force 04.01.2019. Online available: https://www.zakon.hr/z/98/Kazneni-zakon, accessed 31/10/2019.
[155] Zakon o policijskim poslovima i ovlastima, entry into force 01.07.2009. Online available: https://www.zakon.hr/z/173/Zakon-o-policijskim-poslovima-i-ovlastima accessed 31.10.2019.
[156] Pravilnik o načinu postupanja policijskih službenika, entry into force 19.07.2010. Online available: https://narodne-novine.nn.hr/clanci/sluzbeni/2010_07_89_2528.html, accessed 31.10.2019.

d) through the testimony of people who can recognize a person whose identity is being determined through **photos**, film clips, through recognition of clothes, shoes and other items that can be used to determine the identity,

e) using a personal description,

f) by determining the structure of the DNA profile,

g) by other available methods (superposition, graphology expertise, voice analysis, dental formula, etc.).

Article 77 states that The Ministry shall establish at its headquarters: a collection of searches, a collection of notices for people and a collection of notices for cases. **Collection of searches** and collection of notices for people **shall contain the photograph or photorobot of a person**.

6) Biometric Data Processing Law (*Zakon o obradi biometrijskih podataka*)[157]. According to Articles 1 and 2 this Law regulates the processing of biometric data collected by the competent authorities in order to effectively identify and protect natural persons from misuse of their personal data. Article 3 sets out the meanings of important terms for instance: '***Biometric information***' means personal data obtained through special technical processing relating to an individual's physical or physiological characteristics that enable or confirm the unique identification of that individual, such as papillary fingerprints, palms and feet, **photographs**, **facial views**, DNA profile and iris of the eye; '***Face view***' **is a digital face view whose resolution and quality are sufficient for automated biometric matching**; '*Competent authorities*' authorized to collect and process biometric data and establish appropriate data collections referred to in Article 6 of this Law are the ministries competent for internal affairs, foreign affairs, justice affairs and the ministry competent for defense affairs in the part related to conducting military police tasks in accordance with special regulations. According to Article 6 (2) biometric data from the collections established by the competent authorities shall be processed and collected:

1. During the process of issuing personal identification documents, regardless of nationality;
2. **During criminal investigations**, regardless of nationality;
3. **From prisoners and convicts**, regardless of nationality;
4. **Of the perpetrators of the criminal offenses pursued**, regardless of their nationality;
5. Of missing persons, regardless of nationality;
6. From persons who do not have personal identification documents, after establishing such a fact, regardless of citizenship;
7. Of unidentified remains;

[157] Zakon o obradi biometrijskih podataka, effective from 04/01/2020. Online available: https://www.zakon.hr/z/2431/Zakon-o-obradi-biometrijskih-podataka. Added as an exception after 31.10.2019 while other legal acts of this current report have been used in the wording as at 31/10/2019 the latest.

8. From third-country nationals or stateless persons who reside illegally in the Republic of Croatia, who do not have an identity document or their identity is suspected, and from a third-country national in the process of forced removal;
9. From third-country nationals or stateless persons who have indicated their intention to apply for international protection;
10. From third-country nationals or stateless persons applying for a visa;
11. From third-country nationals or stateless persons crossing the national border when registering entry and exit information;
12. When refusing entry to the Republic of Croatia to third-country nationals or stateless persons.
Article 25 stipulates that the Minister responsible for internal affairs shall adopt the ordinance the manner of processing biometric data and the powers to use the system within six months from the day the Law enters into force.

List of legal acts regarding detention of the persons, which regulate the collection and use of facial images in Croatia, are the following:
1) The Execution of Prison Sentence Act (*Zakon o izvršavanju kazne zatvora*)[158].
According to Article 59 the **prisoner shall be photographed even without the prisoner's consent**;
2) Regulations on Admission and Treatment of Arrested Persons and Detainees and on Records Regarding Detainees in Police Units (*PRAVILNIK O PRIJAMU I POSTUPANJU S UHIĆENIKOM I PRITVORENIKOM TE O EVIDENCIJI PRITVORENIKA U PRITVORSKOJ POLICIJSKOJ JEDINICI*)[159]. According to Article 34 the records of arrested and detained persons are kept on the Ministry of the Interior's Information System shall contain information on the identity of the arrested person / detainee and his / her **photograph.**

List of legal acts about issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Croatia, are the following:
1) Law on Travel Documents of Croatian Nationals (*Zakon o putnim ispravama hrvatskih državljana*)[160];
2) Personal Identity Card Act (*Zakon o osobnoj iskaznici*)[161];

[158] Zakon o izvršavanju kazne zatvora, this version entry into force 01.01.2020. Online available: https://www.zakon.hr/z/179/Zakon-o-izvr%C5%A1avanju-kazne-zatvora, accessed 31.10.2019.
[159] PRAVILNIK O PRIJAMU I POSTUPANJU S UHIĆENIKOM I PRITVORENIKOM TE O EVIDENCIJI PRITVORENIKA U PRITVORSKOJ POLICIJSKOJ JEDINICI, entry into force 2019. Online available: http://www.propisi.hr/print.php?id=9465, accessed 31.10.2019.
[160] Zakon o putnim ispravama hrvatskih državljana, entry into force 01.08.2015. Online available: https://www.zakon.hr/z/448/Zakon-o-putnim-ispravama-hrvatskih-dr%C5%BEavljana, accessed 31.10.2019.
[161] Zakon o osobnoj iskaznici, entry into force 06.06.2015. Online available: https://www.zakon.hr/z/447/Zakon-o-osobnoj-iskaznici, accessed 31.10.2019.

3) Regulations on Driving Licenses (*PRAVILNIK O VOZAČKIM DOZVOLAMA*)[162];

4) Regulations on the Form and Content of the Military Identification Card (*PRAVILNIK O OBLIKU I SADRŽAJU IDENTIFIKACIJSKE VOJNE ISKAZNICE*)[163].

In addition to the above-mentioned acts the Law on the Nationals of Member States of the European Economic Area and their families (*Zakon o državljanima država članica Europskog gospodarskog prostora i članovima njihovih obitelji*)[164] and the Immigration Law (*Zakon o strancima*)[165] regulate the collection and use of facial images.

According to legal acts regarding offence proceedings the facial images are collected from the following groups of persons:

1) Based on Law on the Protection of Natural Persons Regarding the Processing and Exchange of Personal Data for the Purpose of Preventing, Investigating, Detecting or Prosecuting Criminal Offenses or Executing Criminal Sanctions:

- persons suspected of having committed or are about to commit a criminal offence;
- persons convicted of a criminal offence legally binding;
- victims of the crime;
- persons who have a knowledge of the crime committed;

2) Based on Regulations on Admission and Treatment of Arrested Persons and Detainees and on Records Regarding Detainees in Police Units:

- arrested;
- detainees;

3) Based on The Execution of Prison Sentence Act – prisoners;

4) Based on Criminal Procedure Code – suspects, defendants.

The purposes to use facial images according to the Criminal Procedure Code and Law of the Police Actions and Authorities are:

1) to investigate a crime;

---

[162] PRAVILNIK O VOZAČKIM DOZVOLAMA, entry into force 2019. Online available: http://www.propisi.hr/print.php?id=7651%20, accessed 31.10.2019.

[163] PRAVILNIK O OBLIKU I SADRŽAJU IDENTIFIKACIJSKE VOJNE ISKAZNICE, entry into force 2014. Online available: http://www.propisi.hr/print.php?id=9147, accessed 31.10.2019.

[164] Zakon o državljanima država članica Europskog gospodarskog prostora i članovima njihovih obitelji, entry into force 18.07.2019. Online available: https://www.zakon.hr/z/2109/Zakon-o-dr%C5%BEavljanima-dr%C5%BEava-%C4%8Dlanica-Europskog-gospodarskog-prostora-i-%C4%8Dlanovima-njihovih-obitelji, accessed 31.10.2019.

[165] Zakon o strancima, entry into force 26.05.2018. Online available: https://www.zakon.hr/z/142/Zakon-o-strancima, accessed 31.10.2019.

2) to establish the identity of the suspect.

According to the Article 34 of Regulations on Admission and Treatment of Arrested Persons and Detainees and on Records Regarding Detainees in Police Units the data of the arrested and detained persons are kept on the Ministry of the Interior's Information System.

Law on the Police Actions and Authorities (Article 25) and Criminal Procedure Code (Article 186) allow to use data, including facial images, which has been collected for other (civil) purposes to be used in offence proceedings.

Cross-border cooperation in case of exchanging evidences is possible between the countries (government entities) according to the Article 188a of the Criminal Procedure Code, the Law on Judicial Cooperation in Criminal Matters with the EU Member States[166] and Article 24(3) of the Law on the Police Actions and Authorities.

3.7. Denmark

In accordance with Articles 2 and 2a of Protocol No. 22 on the position of Denmark, as annexed to the Treaty on European Union (the TEU) and the Treaty on the Functioning of the European Union (the TFEU), Denmark is not bound by the rules laid down in Directive (EU) 2016/680 or subject to their application which relate to the processing of personal data by Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. Given that Directive (EU) 2016/680 builds upon the Schengen acquis, under Title V of Part Three of the TFEU, Denmark, in accordance with Article 4 of that Protocol, had to decide within 6 (six) months after adoption of Directive (EU) 2016/680 whether to implements it in Danish national law.[167]

The following legal acts regarding offence proceedings regulate the collection and use of facial images in Denmark:

[166] Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije, entry into force 01.08.2019. Online available: https://www.zakon.hr/z/345/Zakon-o-pravosudnoj-suradnji-u-kaznenim-stvarima-s-dr%C5%BEavama-%C4%8Dlanicama-Europske-unije, accessed 31.10.2019.
[167] Recital 100 of Directive (EU) 2016/680.

1) The Administration of Justice Act (*Retsplejeloven*)[168]. According to § 776a Prison and Probation Service can **photograph** and record fingerprints of detainees for later identification. *The* Minister of Justice may lay down rules on the conduct of photography and recording of fingerprints, including on storage and destruction. § 791 states that tape recordings, photocopies or other reproduction of what has become known to the police by the intervention must be destroyed if no charge is brought against anyone for the offense which formed the basis of the intervention or if his charges are later abandoned. Section 791a stipulates that the police may take photographs or observe by means of binoculars or other apparatus of persons located in a location not accessible (observation), if :
1) the intervention is considered to be of material importance to the investigation; and
2) the investigation relates to an offense that may result in imprisonment under the law.

However, **the use of a remote controlled or automatically operated television camera, photographic apparatus** or similar apparatus **may only be carried out if the investigation relates to an offense which, by law, may result in imprisonment for one year and six months or more**. According to § 792d body inspections that do not require undressing, **including taking photographs**, prints and inspecting clothing, may be made to a person who is not charged if the investigation relates to an offense which, by law, may result in imprisonment for 1 year and 6 months or more. § 792f states that the police may not store personal photographs for later identification of persons who have not been charged or who have been acquitted or against whom a charge has been filed.

2) The Act relating to the execution of sentences (Bekendtgørelse af lov om fuldbyrdelse af straf m.v.)[169]. According to § 61 of this law, the Prison and Probation Area has the right to **photograph** and record fingerprints of the inmate for later identification.

3) The Law Enforcement Act (*Lov om retshåndhævende myndigheders behandling af personoplysninger*)[170]. The Act applies to the police, the prosecutor's office, including the military prosecutor's office, the criminal justice service, the Independent Police Accounting Authority and the courts' processing of personal data that is wholly or partially processed by means of automatic data processing and for other non-automatic processing of personal data that is or will be contained in a register when processing is conducted for the purpose of preventing, investigating, detecting or

[168] Bekendtgørelse af lov om rettens pleje, no. 938 of 10 September 2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=209542, accessed 31/10/2019.
[169] Bekendtgørelse af lov om fuldbyrdelse af straf m.v., no. 1333 of 9 December 2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=210247, accessed 31/10/2019.
[170] Lov om retshåndhævende myndigheders behandling af personoplysninger, no. 410 of 27 April 2017. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=189891, accessed 31/10/2019.

prosecuting criminal acts or enforcing criminal penalties, including to protect against or prevent threats to public safety. According to Section 3 Biometric data is personal data which, as a result of specific technical processing regarding the physical, physiological or behavioral characteristics of a natural person, enable or confirm a unique identification of the person, e.g. **face image** or fingerprint information.

4) Order on photography and recording of fingerprints of prisoners in the institutions of the Prison and Probation Service (*Bekendtgørelse om fotografering og optagelse af fingeraftryk af indsatte i kriminalforsorgens institutioner*)[171]. According to § 1 the Prison and Probation Area has the right to photograph and record fingerprints of the inmate for identification. § 2 stipulates that the Prison Area shall ensure that the inmate is re-photographed when (1) it is necessary for later identification; or 2) that person has been deployed for 1 year, and then every year.

5) The legal act regarding the detention of persons, which regulates the collection and use of facial images in Denmark, is: The Danish order on detention (*Bekendtgørelse om ophold i varetægt*)[172]. According to § 85 the Prison and Probation Area has the right to photograph a detainee for later identification.

List of legal acts on the issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Denmark:
1) Order on passports (*Bekendtgørelse om pas m.v.*)[173]
2) Order on driving licenses (*Bekendtgørelse om kørekort*)[174] and the Traffic act (*Færdselsloven*[175]).
3) Law on the issueance of identification cards (*Lov om udstedelse af legitimationskort*)[176] and order on the issuance of identification cards (Bekendtgørelse om udstedelse af legitimationskort)[177].

---

171 Bekendtgørelse om fotografering og optagelse af fingeraftryk af indsatte i kriminalforsorgens institutioner (fotobekendtgørelsen), no 109 of 30 January 2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=206605, accessed 31/10/2019.
172 Bekendtgørelse om ophold i varetægt, no. 107 of 30 January 2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=206603, accessed 31/10/2019.
173 Bekendtgørelse om pas m.v.), no. 1337 of 28 November 2013. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=159226, accessed 31/10/2019.
174 Bekendtgørelse om kørekort, no. 27 August 2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=210058, accessed 31/10/2019.
175 Færdselsloven, no. 1324 of 21 November 2018. Online available: https://www.retsinformation.dk/forms/R0710.aspx?id=204976, accessed 31/10/2019.
176 Lov om udstedelse af legitimationskort, no. 236 of 15 March 2017. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=187037, accessed 31/10/2019.
177 Bekendtgørelse om udstedelse af legitimationskort, no. 1220 of 21 November 2017. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=194777, accessed 31/10/2019.

In addition to the abovementioned acts, the Aliens Act (*Bekendtgørelse af udlændingeloven*)[178] regulates the collection and use of facial images.

According to legal acts regarding offence proceedings, facial images are collected from the following groups of persons:

1) Accused, suspects, a person requested in an arrest warrant (based on the Administration of Justice Act);

2) Inmates (based on the Act relating to the execution of sentences, section 61);

3) The data subject (based on the Law Enforcement Act);

4) Inmates (based on the order on photos);

5) Prisoners in custody (based on the order on detention).

The purposes of using facial images according to the following legal acts are:

1) The Administration of Justice Act – to investigate a crime, perform procedures and identification;

2) The Act relating to the execution of sentences and Order on photos – for identification purposes and to perform procedures;

3) The Law Enforcement Act – processing of personal data;

4) Order on passports and the Law on the issue of identification cards – to grant an identity document and identification purposes.

5) Order on driving licenses – identification purposes and proof of ability to drive.

6) Aliens Act – to grant an identity document and perform procedures.

According to the laws, facial images are stored in following databases:

1) The National Danish Photo Registry administered by the police (based on the Administration of Justice Act)

2) The Central Passport Register (based on the Order on passports)

3) The Central Driving License register (based on the Order on driving licenses).

The Administration of Justice Act and the Law Enforcement Act allow the use of data, including facial images, which have been collected for other (civil) purposes to be used in offence proceedings.

[178] Bekendtgørelse af udlændingeloven, no. 1022 of 2 October 2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=210545, accessed 31/10/2019.

Cross-border cooperation in the case of exchanging personal data (including facial images) is possible between countries (government entities) according to the Law Enforcement Act Chapter 16.

3.8. Estonia

The Estonian legal system is based on the Continental European civil law model and has been influenced by the German legal system.[179] Consolidated texts of English translations of Estonian legislation can be found online.[180] "The central information system – e-File – provides an overview of the different phases of criminal, misdemeanour, civil and administrative procedures, court adjudications and procedural acts to all parties involved, including the citizen."[181]

Relevant laws regarding offence proceedings which regulate the collection and use of facial images in Estonia are the Code of Criminal Procedure [182], Code of Misdemeanour Procedure [183] and Law Enforcement Act[184].

§ 15^2 (1) ('processing of personal data in criminal procedure') of the Code of Criminal Procedure stipulates that in criminal proceedings, the body conducting proceedings has the right to process personal data, including personal data of specific categories, which are required for conduct of pre-trial proceedings and judicial proceedings, taking of evidence, enforcement of the decisions made in criminal matters, conduct of surveillance activities or achievement of other objectives provided for in the Code of Criminal Procedure. Subsection (2) of the same paragraph adds that when processing personal data in the course of criminal proceedings, the body conducting proceedings acts as a law enforcement authority for the purposes of subsection 13 (2) of the Personal Data Protection Act, and the processing of personal data is guided by the provisions established for law enforcement authorities. § 15^2 (3) of the Code of Criminal Procedure refers that exercise of the rights of data subjects arising from the Personal Data Protection Act is guided by the provisions of the Code of Criminal Procedure, regardless of whether the

[179] https://investinestonia.com/business-in-estonia/legal-system/ , accessed 30.11.2019.
[180] https://www.riigiteataja.ee/en/, accessed 30.11.2019.
[181] https://e-estonia.com/solutions/security-and-safety/e-justice/, accessed 30.11.2019.
[182] Code of Criminal Procedure, entry into force 01.07.2004, online available: https://www.riigiteataja.ee/en/eli/ee/508042019008/consolide/current , EN, accessed 14.10.2019.
[183] Code of Misdemeanour Procedure, entry into force 01.09.2002, online available: https://www.riigiteataja.ee/en/eli/508042019014/consolide , EN, accessed 14.10.2019.
[184] Law Enforcement Act, entry into force 01.07.2014, online available: https://www.riigiteataja.ee/en/eli/525032019010/consolide , EN, accessed 14.10.2019.

data subject is a suspect, accused, victim, civil defendant, third party, witness or any other person. Subsection (4) of the same paragraph states that when processing personal data pursuant to the Code of Criminal Procedure, a data controller may restrict the rights of a data subject arising from the Personal Data Protection Act if this is required in order to prevent, detect, proceed an offence or enforce a punishment, conduct civil, administrative or any other legal proceedings, prevent any damage to the rights and freedoms of another person or data subject, prevent endangering of national security or ensure maintenance of public order.

Evidence, according to the Code of Criminal Procedure, means the statements of a suspect, accused, victim, the testimony of a witness, an expert's report, the statements given by an expert upon provision of explanations concerning the expert's report, physical evidence, reports on investigative activities, minutes of court sessions and reports or video recordings on surveillance activities and other documents, photographs, films or other data recordings.[185]

§ 31 (1^1) ('Collection of evidence and application of provisions of criminal procedure in performance of procedural acts') of the Code of Misdemeanour Procedure states that if the time, place or manner of commission of a misdemeanour or other facts relating to the misdemeanour have been **photographed** or video recorded in the course of state supervision, this recording may be independent evidence in misdemeanour proceedings if the following appears from the recording:

1. the connection of the recording with the misdemeanour
2. when, on what grounds and by whom the recording was created
3. other facts relevant for resolving the misdemeanour matter

Photographs, films or other data recordings made by a body conducting proceedings may be independent evidence in misdemeanour proceedings if they conform to the provisions brought out in the previous paragraph (clauses 31 (1^1) 1) to 3) of the Code of Misdemeanour Procedure).[186]

The police or, in the cases provided by law, another law enforcement agency may, with the knowledge of the person, establish identity on the basis of a valid identity document, i.e. ascertain the person's name and personal identification code or in the absence of the latter the date of birth, examine the document, compare the **photograph and other biometric data** in the document with the person, and verify the authenticity of the document, or if this is not possible, establish identity in another legal manner if it is

[185] § 63 of the Code of Criminal Procedure.
[186] § 31^4 of the Code of Misdemeanour Procedure.

necessary for preventing, ascertaining or countering a threat or eliminating a disturbance.[187] For the establishment of identity, the police or, in the cases provided by law, another law enforcement agency has the right to stop a person and require them to present a document specified in the previous sentence (§ 32(1) of the Law Enforcement Act), to obtain statements enabling the establishment of identity, including information on the person's place of residence, and to obtain biometric data for the comparison specified in the previous sentence (§ 32(1) of the Law Enforcement Act).[188]

The legal regulations regarding the detention of persons regulating the collection and use of facial images are the Imprisonment Act[189] and Aliens Act[190].

A person who is received into a prison for serving a sentence is **photographed** and fingerprinted and their DNA sample is collected for the purposes of identification of the person, detection and prevention of offences, unless these acts have been carried out during the custody pending trial or earlier in the course of criminal proceedings.[191]

The signaletic photographs of a prisoner are annexed to the personal file of the prisoner. One set of signaletic photographs is sent to the investigative body which requested that the person be taken into custody where it is annexed to the criminal file.[192]

Specifications under the Alien Act, which regulates the bases for the entry of aliens into Estonia, their temporary stay, residence and employment in Estonia and their legal liability for violation of obligations provided for in the Aliens Act, for taking biometric data from persons staying in a custodial institution: if in the course of the proceeding arising from the Aliens Act, the taking of biometric data from a foreigner is prescribed, an administrative authority may take biometric data from a prisoner or a person in detention or custody staying in a custodial institution in Estonia in the custodial institution.[193] **For the purposes of the Aliens Act, biometric data is a facial image, fingerprint images, a signature or an image of a signature and iris images.**[194]

---

[187] § 32(1) of the Law Enforcement Act.
[188] § 32(2) of the Law Enforcement Act.
[189] Imprisonment Act, entry into force 01.12.2000, online available: https://www.riigiteataja.ee/en/eli/ee/520062019002/consolide/current, EN, accessed 14.10.2019.
[190] Aliens Act, entry into force 01.10.2010, online available: https://www.riigiteataja.ee/en/eli/ee/529032019002/consolide/current, EN, accessed 14.10.2019.
[191] § 18(1) of the Imprisonment Act.
[192] § 18(2) of the Imprisonment Act.
[193] § 279[1] of the Aliens Act.
[194] § 272 (2) of the Aliens Act.

The legal regulations in Estonia regarding the issuance and use of identity documents regulating the collection and use of facial images are: the Identity Documents Act[195], the Standard format and technical description of an identity card and a list and the period of validity of digital data entered on an identity card [196] and the Traffic Act[197]. An identity document is a document issued by a state authority on which the name, date of birth or personal identification code and a photograph or facial image and the signature or an image of the signature of the holder are entered, unless otherwise provided for by law or legislation established on the basis thereof.[198] According to point 1 of § 4 (2) of the Standard format and technical description of an identity card and a list and the period of validity of digital data entered on an identity card, the identity card must have on the front side of the identity card the facial image of the holder of the identity card.

The Road Administration has the right to take biometric data (**facial image,** fingerprint images, the signature or signature image and eye iris images) and process these in the course of the proceedings related to the application and issue of the documents certifying the right to drive.[199]

According to the Code of Criminal Procedure[200] and Imprisonment Act,[201] **facial images** can be collected from Suspects, Accused, Victims, Civil defendants, Witnesses, Prisoners, Persons in custody, Detained persons in Detention Houses and/or any other persons. § 15^2 (3) of the Code of Criminal Procedure brings out that the exercise of the rights of data subjects arising from the Personal Data Protection Act is guided by the provisions of the Code of Criminal Procedure, regardless of whether the data subject is a suspect, accused, victim, civil defendant, third party, witness or any other person.

There are no specific laws that concretely refer to the purposes for which the use of facial images is allowed. For that reason, provisions on evidence and data protection, referred to in different laws, should be taken into account and followed. If the time, place or manner of commission of a misdemeanour or other facts relating to the misdemeanour have been photographed or video recorded in the course of

[195] Identity Documents Act, entry into force 01.01.2000, online available: https://www.riigiteataja.ee/en/eli/529032019005/consolide, EN, accessed 14.10.2019.
[196] Standard format and technical description of an identity card and a list and the period of validity of digital data entered on an identity card, passed 02.11.2018 no 27, online available: https://www.riigiteataja.ee/akt/109112018005, ET, accessed 14.10.2019.
[197] Traffic Act, entry into force 01.07.2011. online available: https://www.riigiteataja.ee/en/eli/525032019002/consolide, accessed 14.10.2019.
[198] § 2 of the Identity Documents Act
[199] § 175 (4) of the Traffic Act
[200] Code of Criminal Procedure. Op.cit.
[201] Imprisonment Act. Op.cit.

state supervision, this recording may be independent evidence in misdemeanour proceedings if the following appears from the recording:

1) the connection of the recording with the misdemeanour
2) when, on what grounds and by whom the recording was created
3) other facts relevant for resolving the misdemeanour matter[202]

The submission of information collected pursuant to the Security Authorities Act as evidence in criminal proceedings is decided by the Prosecutor General taking into account the restrictions specified in subsections 126[1] (2) and 126[7] (2) of the Code of Criminal Procedure.[203] Evidence not listed in subsection (1) of § 63 may also be used in order to prove the facts relating to criminal proceedings, except in cases when the evidence has been obtained by way of a criminal offence or violation of a fundamental right.[204]

The national databases in which facial images are stored and processed are, for example:

- Identity documents database (Statutes of the identity documents database[205])
- Border control database (Statutes of the border control database[206])
- Database of border crossing queue (Statutes of the database of border crossing queue[207])
- Database of prisoners, detained persons, persons in custody and probationers (Statutes of the database of prisoners, detained persons, persons in custody and probationers[208])
- State Register of Schengen Information System (Statutes of the State Register of Schengen Information System[209])
- Police database (Statutes of the police database[210])
- Database of aliens staying or having stayed in Estonia illegally (Statutes for maintaining the database of aliens staying or having stayed in Estonia illegally[211])

[202] § 31 of the Code of Misdemeanour Procedure.
[203] § 63 (1[1]) of the Code of Criminal Procedure.
[204] § 63 (3) of the Code of Criminal Procedure.
[205] Statutes of the identity documents database, entry into force 01.01.2016, online available: https://www.riigiteataja.ee/akt/102022018003, ET, accessed 14.10.2019.
[206] Statutes of the border control database, entry into force 12.01.2008, online available: https://www.riigiteataja.ee/akt/112032019040, ET, accessed 14.10.2019.
[207] Statutes of the database of border crossing queue, entry into force 15.08.2010, online available: https://www.riigiteataja.ee/akt/118092018010, ET, accessed 14.10.2019.
[208] Statutes of the database of prisoners, detained persons, persons in custody and probationers, passed 01.03.2018 no 19, online available: https://www.riigiteataja.ee/akt/109032018003, ET, accessed 14.10.2019.
[209] Statutes of the State Register of Schengen Information System, entry into force 01.01.2010, online available: https://www.riigiteataja.ee/akt/112032019038, ET, accessed 14.10.2019.
[210] Statutes of the police database, entry into force 01.01.2010, online available: https://www.riigiteataja.ee/akt/112032019039, ET, accessed 14.10.2019.
[211] Statutes for maintaining of database of aliens stayng or having stayed in Estonia illegally, entry into force 01.10.2010, online available: https://www.riigiteataja.ee/akt/128102016010, ET, accessed 14.10.2019.

- Database of persons who have acquired or lost Estonian citizenship or to whom Estonian citizenship has been restored (Statutes of the database of persons who have acquired or lost Estonian citizenship or to whom Estonian citizenship has been restored[212]).

In addition to the above, it should be brought out that **facial images could be uploaded to the e-file system.** E-File is an online information system which allows procedural parties and their representatives to electronically submit procedural documents to courts and observe the progress of the proceedings related thereto.[213] Moreover, it should be brought out that X-road is the backbone of the Estonian State because the absolute majority of registers and databases kept by the Estonian State are made available via X-road.[214] Without X-road, if the State wanted to store and exchange its data, it would have to build a Central SuperDatabase or establish a horse-sleigh company to move data storage devices between municipalities and agencies across Estonia.[215]

Transfer of evidence to other EU Member States is possible according to §489[48] of the Code of Criminal Procedure, which states that the Prosecutor's Office immediately transfers to the requesting Member State the evidence obtained on the basis of the European Investigation Order in the possession of the Prosecutor's Office or investigative body and the evidence obtained as a result of execution of the European Investigation Order.[216] Transfer of evidence may be suspended until the end of the proceedings on appeal if the procedural act by which the evidence was obtained has been contested pursuant to this Code. Transfer of evidence may not be suspended if sufficient reasons are stated in the European Investigation Order that immediate transfer of evidence is essential for proper performance of the procedural act or protection of the rights of individuals, except in cases when the transfer of evidence may result in a serious and irreversible violation of the rights of persons.[217] In agreement with the competent authorities of the requesting Member State, the Prosecutor's Office may temporarily transfer the evidence requested provided that the evidence is returned to Estonia as soon as these are no longer required in the requesting Member State, or at any other time agreed upon between the Prosecutor's Office and the competent authorities of the requesting Member State.[218]

It appears that use of facial images and facial recognition in offence proceedings is not directly or clearly regulated in Estonia. The legal basis for having such data base for facial images is therefore also missing.

[212] Statutes of the database of persons who have acquired or lost Estonian citizenship has been restored, passed 18.12.2015 nr 75, online available: https://www.riigiteataja.ee/akt/129122015001, ET, accessed 14.10.2019.
[213] https://www.rik.ee/en/e-file, accessed 30.11.2019.
[214] https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html, accessed 30.11.2019.
[215] Ibid.
[216] §489[48](1) of the Code of Criminal Procedure.
[217] §489[48](2) of the Code of Criminal Procedure.
[218] §489[48](3) of the Code of Criminal Procedure.

It appears that the Ministry of Interior Affairs of Estonia has a plan to create an Automatic Biometric Identification System (ABIS), which enables biometric data to be taken and stored and data to be compared (one to one and one to many). Furthermore, this system will be connected to other systems which need biometric identification.[219]

3.9. Finland

There are some opinions in Finland that Finnish Constitution does not allow the limitation of the right to privacy on the basis of precautionary security, such as extensive surveillance legislation. Some scholars are in opinion that the Finnish Constitution needs to be amended for that. However, the Finnish Constitutional Law Committee has been in opinion that there is no obstacle to the retention of personal data, if the proportionality requirements are met in other ways.[220]

In Finland, in addition to the national law, the National Police Board and the Ministry of the Interior Affairs have enacted over hundred different manuals, handbooks and orders to instruct police work. These manuals are available to every police officer in the police online system called Sinetti, but perhaps due to vast amount of these handbooks and continuously changing regulations, these are not circulated among the officers when enacted or amended. In practice, it is impossible for every police officer to know and apply these orders and manuals although it is crucial to know how personal data and privacy are protected.[221] Most of the work appears to be on paper and signed manually as electronic signature is not in place.

The processing of personal data must comply with the requirement of respect for fundamental rights and human rights as set out in Chapter 1 of the Police Act (872/2011), the principle of proportionality, the principle of minimum harm and the principle of purpose limitation.[222]

[219] Siseministeerium, Biomeetriliste andmete kasutamise kontseptsioon. Op.cit.
[220] N. Vainio. Fundamental rights Compliance and the politics of interpretation: Explaining Member State and court reactions to Digital Rights Ireland. T. Bräutigam & S. Miettinen, Data Protection, Privacy and European Regulation in the Digital Age, p 229-260. Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, 2016.
[221] L.J. Pajunoja. The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU's data protection law and its compatibility with the right to privacy. University of Helsinki, Faculty of Law, 2017, p 71-72.
[222] Poliisilaki 872/2011 Chapter 1

In Finland, the processing of personal data must not be based on an unacceptable basis based on the age, sex, origin, nationality, place of residence, language, religion, belief, opinion, political activity, trade union activity, family relationships, health status, disability, sexual orientation or other person-related cause.[223]

In general, misuse of facial images, such as publishing facial images with insulting texts, might lead one to commit defamation of character has and as a consequence the punishment of fine (felony: fine or time in prison max. 2 years).[224]

Shortly, the Finnish Act on the processing of personal data by the police (616/2019) sets rules for national police when it is exchanging data with foreign countries and other law enforcement officers. Personal data might be given e.g. to Europol, Eurodac system and national authorities such as prosecutors, courts or customs. Act has reference to Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018)[225] in which Chapter 7 there are more specific rules in which circumstances personal data may be disclosed to third countries and international organizations.

Facial recognition in offence proceedings

Current situation

The Finnish laws enable police to deal with identification data for identification, including audio sample, facial image and other biometric data.[226] Police of Finland has made public Privacy Policies of National Information Systems controlled by the police, which provide all the information necessary to know about how personal data is being processed by them. Facial recognition technology can be used by law enforcement agencies according to the applicable national laws.

In Finland, the police process personal data to perform investigation and supervision duties, to perform their statutory obligations and to exercise their public authority when the conditions laid down in data

[223] Laki henkilötietojen käsittelystä poliisitoimessa, entry into force 01.06.2019, online available: http://www.finlex.fi/fi/laki/alkup/2019/20190616?search%5Btype%5D=pika&search%5Bpika%5D=616%2F2019#Pidp447484848 (28.10.2019)
[224] Finnish Criminal Act Section 24: 9 § and 10 §
[225] Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). English translation of the act: https://www.finlex.fi/fi/laki/kaannokset/2018/en20181054.pdf
[226] Section 8(3) of the Act on the processing of personal data by the police 616/2019

protection legislation are met.[227] "The processing of personal data by the police and the legal basis for such processing is governed by the following laws, among others: The Act on the Processing of Personal Data by the Police (616/2019, hereafter the Police Personal Data Act), the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018, hereafter the Act on Data Protection in Criminal Matters), the Police Act (872/2011), the Police Decree (1080/2013), the Pre-trial Investigation Act (805/2011), the Coercive Measures Act (806/2011), the Decree on Pre-trial Investigation, the Coercive Measures and Covert Data Acquisition (122/2014), and the Act on Background Checks (726/2014), General Data Protection Act EU (2016/679), Data Protection Act (1050/2018)."[228]

The police process personal data specified in the Police Personal Data Act in order to carry out pre-trial investigations and police investigations; to solve crimes; and to perform tasks related to the consideration of filing charges, the maintenance of public order and safety or another supervisory task of the police, provided that the data relates to persons who are

1) suspected of an offence or participation in an offence;
2) under 15 years of age and suspected of an offence;
3) subject to pre-trial investigation, police investigation or a police measure;
4) reporters of an offence or injured parties;
5) witnesses;
6) victims;
7) directly related to field duties or supervisory duties specifically provided
for in legislation; or
8) providers of other further information related to a duty.[229]

In Finland, in addition to basic information on the above-mentioned persons, the police also process identifying information to establish a person's identity, including facial images and other biometric data.[230]

The police may process personal data for the purpose of carrying out a task related to the prevention or detection of criminal offenses, the information referred is related to persons:

[227] National Police Board Privacy statement ID-19209128, available at: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/86226_Processing_of_personal_data_in_investigation_and_supervision_duties.pdf?2b826f39477dd788
[228] Ibid.
[229] Section 5 of the Act on the processing of personal data by the police 616/2019
[230] Section 6 of the Act on the processing of personal data by the police 616/2019

1) who may reasonably be presumed to have committed or are guilty of an offense punishable by law as the most severe offense;
2) who are in contact with, or are in contact with, a person referred to in paragraph 1 and, by reason of their repetition, circumstances or the conduct of a person, may be presumed to be connected with the offense;
3) are subject to surveillance or other police action in accordance with Chapter 5, Section 13 of the Police Act.[231]

The police may deal with the information referred above if it is necessary for the prevention or detection of the crime, including the following persons:

1) witnesses of crime;
2) victims of crime;
3) the offenders or the persons involved in the crime.[232]

"The police process the personal data specified in the Police Personal Data Act in order to carry out tasks related to license administration and such statutory supervisory duties specifically imposed on the police that are not related to the prevention, uncovering or investigation of crimes, to referring investigated offences to a prosecutor for consideration of charges or to protecting the public safety from threats and the prevention of such threats."[233] Police processes photos provided to the police, the Ministry for Foreign Affairs or foreign affairs administration authority when a person applies for a permit or a decision the preparation of which requires the photo, and facial photo taken of the applicant at the time of applying for a passport or identity card in order to carry out the duties laid down in the Identity Card Act (663/2016) and Passport Act (671/2006).[234]

The police may also process personal data for the purpose of authorizing and supervising police activities not specifically provided for by law that do not involve the prevention, detection, detection or prosecution of criminal offenses or threats to public security or the prevention of such threats,[235] that includes facial

[231] Section 7 of the Act on the processing of personal data by the police 616/2019
[232] Section 7 of the Act on the processing of personal data by the police 616/2019
[233] National Police Board Privacy statement ID-19209171, available at: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/86228_Processing_of_personal_data_in_relation_to_other_statutory_tasks_of_the_poli.pdf?df467439477dd788
[234] Ibid.
[235] Section 11 of the Act on the processing of personal data by the police 616/2019

image taken from the applicant for an identity card or passport in order to carry out the tasks provided for in the Identity Card Act (663/2016) and passport law (671/2006).[236]

The police process personal data specified in the Police Personal Data Act for purposes other than the original purpose of processing, taking into consideration the legal restrictions for processing personal data:

1) to prevent or detect a crime;
2) to investigate a crime for which the most severe punishment prescribed by law is imprisonment;
3) to reach the person sought;
4) as a statement supporting innocence;
5) to prevent significant danger to life, health or liberty, or significant damage to the environment or property;
6) to protect national security;
7) for identification purposes, when carrying out a police measure that necessarily requires identification;
8) to guide the police.[237]

Notwithstanding the confidentiality rules, information from the police personal data register may also be processed in law enforcement, analysis, planning and development activities.[238] In addition, the information may be used for training purposes if the information is necessary for the purposes of training.[239] The person's photograph may, with the consent of the person concerned, be used for the preparation of any other administrative authorization or decision sought by him, other than the production of the document to which the photograph and the specimen of the signature have been given.[240]

"The above data is used as a source of information for basic and extended background checks in the manner and to the extent determined in the Act on Background Checks."[241]

Disclosure of personal data by police

[236] Section 12(5) of the Act on the processing of personal data by the police 616/2019
[237] Section 13 of the Act on the processing of personal data by the police 616/2019
[238] Ibid.
[239] Ibid.
[240] Ibid.
[241] Section 13 of the Act on the processing of personal data by the police 616/2019

"The police disclose personal data related to investigation and supervision tasks through a technical interface or as sets of data to the Finnish Security Intelligence Service, Customs, Border Guard, Defense Forces, prosecutors, courts of law, Legal Register Centre, Criminal Sanctions Agency and other competent authorities as specified in the Act on Data Protection in Criminal Matters, for the purpose of performing the statutory duties laid down in section 1 of said Act."[242]

Furthermore, according to Chapter 4 of the act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security, the police may disclose personal data related to other statutory duties of the police through a technical interface or as sets of data to other authorities for the performance of duties laid down in the Act applicable to the authority or pursuant to the Police Personal Data Act or some other Act within the scope and under the permit conditions set out in more detail in separate data permits.

"The police disclose personal data related to the prevention or uncovering of crimes in connection to an individual matters or as a set of data also to competent authorities of member states of the European Union and the European Economic Area that process personal data in order to prevent, investigate or uncover crimes, take legal action in connection to a crime or enforce criminal sanctions. This includes protection from and prevention of threats to general safety. The party obtaining the data has the right to process personal data on the same conditions that the police is allowed to process the data in question.

The police disclose personal data related to prevention and uncovering of crimes in connection to an individual matter or as a set of data to Eurojust and other institutions established on the basis of the Treaty on the Functioning of the European Union, the duties of which include upholding social order and the judicial system, maintaining public order and security or preventing and solving crimes and considering the filing of charges, for the purpose of performing these duties.

The police disclose personal data related to prevention and uncovering of crimes in connection to an individual matter or as a set of data to competent law-enforcement authorities in member states of the European Union at their request, provided that the data and intelligence information are needed to prevent or solve crimes. A competent authority is obliged to disclose the above personal data to a competent law-enforcement authority in charge of criminal investigation or security intelligence in another member country unprompted if the disclosure can be assumed to contribute to the prevention or

[242]Section 21 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018)

solving of crimes as per section 3(2) of the Act on Extradition on the Basis of an Offence Between Finland and Other Member States of the European Union (1286/2003).

The police disclose personal data related to the prevention or uncovering of crimes to the European Union Agency for Law Enforcement Cooperation (Europol) in compliance with the Europol Regulation (EU) 2016/794 and the Act on the European Union Agency for Law Enforcement Cooperation (214/2017).

The police disclose personal data related to the prevention or uncovering of crimes on the basis of the Prüm Convention (54/2007) and the Prüm Decision (2008/615/JHA) to the member states party to the convention and to the extent specified in the Prüm Convention and Prüm Decision, especially to prevent terrorism and cross-border crime.[243]

The police disclose personal data related to the prevention or uncovering of crimes in connection to an individual matter or as a set of data to the International Criminal Police Organization (ICPO-Interpol) on the basis of chapter 7 of the Act on Data Protection in Criminal Matters, for the purpose specified in section 1(1) of said act.[244]

The police disclose personal data related to other statutory duties of the police in connection with an individual matter or as sets of data pursuant to Chapter 7 of the Act on Data Protection in Criminal Matters:
1) personal data to the competent authorities referred to in international agreements or other arrangements concerning the taking back of illegal immigrants and people who are illegally resident, for the purposes of the duties specified in the international agreements and arrangements in question;
2) personal data related to the acquisition, possession, transfer, import and export of firearms, firearm components, cartridges, and particularly dangerous projectiles to authorities responsible for gun control in other countries, provided that the disclosure of information is necessary for gun control.[245]

Biometric data processing is allowed only where it is strictly necessary, subject to appropriate safeguards for the rights of the data subject, and only where the processing: 1) is provided by law; 2) relates to the consideration of a criminal case in the prosecution service or in court; 3) is necessary for protecting a

[243] National Police Board Privacy statement ID-19305711, available at: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/86227_Processing_of_personal_data_in_order_to_prevent_or_uncover_crimes.pdf?891e0223a279d788
[244] National Police Board Privacy statement. Op.cit.
[245] Section 31 of the Act on the processing of personal data by the police 616/2019

vital interest of the data subject or of another natural person; or 4) relates to data which the data subject has manifestly made public.[246]

According to Section 41 of Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security a competent authority may transfer personal data to a third country or an international organization only if the other provisions applicable to the processing of personal data referred to in this Act are complied with and if

1) the transfer is necessary for a purpose mentioned in section 1, subsection 1[247];

2) the personal data are transferred to a controller in a third country or to an international organization which is competent to process personal data for a purpose mentioned in section 1, subsection 1; and

3) a valid decision of the European Commission (the Commission) on the adequacy of the level of protection referred to in article 36 of the Law Enforcement Directive exists, or unless such a decision exists, appropriate safeguards exist as provided in section 42 of this Act, or if the derogations for specific situations under section 43 are applicable.

According to section 42 personal may be transferred also based on appropriate safeguards. If the Commission has not made a decision referred to in section 41, subsection 1, paragraph 3, personal data may be transferred to a third country or an international organization if the other conditions laid down in section 41 are met and

1) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

2) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

The controller shall inform the Data Protection Ombudsman about the categories of the transfers made under subsection 1, paragraph 2. The following information on the transfers shall be documented and, on request, made available to the Data Protection Ombudsman:

1) the date and time of the transfers;

2) the receiving competent authority;

3) the justification for the transfers; and

4) the personal data transferred.

[246] Section 11of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). Available at: https://www.finlex.fi/en/laki/kaannokset/2018/en20181054.pdf

[247] Purposes mentioned in section 1 subsection 1 are: preventing, detecting or investigating criminal offences or referring them for consideration of charges.

It is stipulated in section 43 of the aforementioned act the specific situation when the data may be enclosed as well even if the aforementioned criteria(s) are not met, such as the transfer of personal data is required in order to protect the vital interests of the data subject or another person. In section 44 it is stipulated the special circumstances in which personal data may be enclosed to private entities and other recipients established in third countries.

Databases of facial images that will be used for facial recognition in offence proceedings and deletion of the personal data

"The Population Information System is one of the most central databases in Finland. It contains up-to-date information on all Finnish citizens as well as foreigners living permanently in Finland. The system is maintained by the Population Register Centre and the local register offices."[248]

Data concerning individuals who have been subject to a security clearance vetting according to the Security Clearance Act is stored in the security clearance register.[249] Provisions on the handling of personal data stored in the security clearance register are laid down in the Security Clearance Act (726/2014) and in the Act on the Handling of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018).[250]

The Legal Register Centre is an agency in the administrative sector of the Ministry of Justice whose function is to act as the controller for information systems and registers; to be responsible for enforcement tasks relating to fines, forfeitures, payments and claims; to be responsible for maintaining and developing information systems.[251] The Finnish Legal Register Centre is tasked with register-keeping and data management of the administrative branch of the Ministry of Justice's key registers, for example criminal records are kept in a national central register.[252]

Information about distinctive identifiers used to verify identity will be deleted no later than ten years after the last entry regarding the person suspected of a crime was made. However, information will be deleted

[248] Population Register Centre, available at: https://vrk.fi/en/check-your-registered-data-
[249] Finnish Security Intelligence Service (Supo), Data Protection and Handling of Personal Data, available at: https://www.supo.fi/security_clearances/security_clearance_register/data_protection
[250] Ibid.
[251] Legal register centre, available at: https://www.suomi.fi/organization/legal-register-centre/eddf8635-77ba-4e85-b136-1be460750de7
[252] Legal Register Centre (LRC), available at: https://www.oikeusrekisterikeskus.fi/en/index/loader.html.stx?path=/channels/public/www/ork/en/structured_nav/oikeusrekisterikeskus

no later than ten years after the death of the data subject if the maximum punishment for the grossest offence used as basis for registration is no less than one year of imprisonment.

Information about distinctive identifiers used to verify identity, as well as information about distinctive identifiers of persons who were under 15 years of age at the time of the offence, will be deleted no later than one year after the entry was made, if investigation proves that no offence was committed or that there is no longer reason to suspect the person of the crime.

The above-mentioned personal data related to a criminal case may be retained for a longer period if it is needed for investigation or supervision purposes or other justified purposes or to safeguard the rights of the data subject, another party or a member of the police personnel. The necessity of the further retention of personal data must be evaluated at intervals of five years or less."[253]

"Personal data processed in order to find missing persons or identify unidentified deceased persons will be deleted no earlier than five years after the missing person was found or the deceased person identified; however, information on close relatives required in finding people reported missing and identifying unidentified deceased persons will be deleted at the data subject's request or as soon as the information is no longer needed for its processing purpose; and information on personal identifiers and travel document information processed in order to perform tasks specified in section 131 of the Aliens Act will be deleted ten years after the last entry regarding the data subject was made; if the data subject is granted Finnish citizenship, the information will be deleted one year after the controller received information about the granting of citizenship.

Information on personal identifiers and travel document information processed in order to perform tasks specified in section 131 of the Aliens Act, as well as the safety data of persons subject to measures related to investigation and supervision duties, will be deleted no later than one year after the death of the data subject.

However, the above-mentioned personal data may be retained for a longer period if it is needed for investigation or supervision purposes or other justified purposes or to safeguard the rights of the data subject, another party or a member of the police personnel. The necessity of the further retention of personal data must be evaluated at least every five years." [254]

[253] National Police Board Privacy statement ID-19209128
[254] National Police Board Privacy statement. Op.cit.

Facial recognition searches

On 11th of March 2019, Finnish Parliament approved a government proposal for a Civilian Intelligence Act, which will enhance the surveillance capabilities of military and civil intelligence agencies. „The new civilian intelligence powers may only be used by the Finnish Security Intelligence Service and they can also be exercised abroad. In future, the basis for information gathering by the Finnish Security Intelligence Service will be not only the prevention and detection of crime but also national security. The focus of information gathering by the Finnish Security Intelligence Service will be on detecting threats and responding to them at an earlier stage than has been previously possible."[255] The use of automatic facial recognition technology is enabled with the new law, which allows authorities to compare people's faces captured by surveillance cameras to images of individuals stored in official databases and will enhance the surveillance capabilities of military and civil intelligence agencies. Finnish Border Guard had the right to use such technology since 2005[256].

Although the permission to use technology exists to use the software for automatic facial recognition, Finland's current technological infrastructure doesn't support it. Automatic face detection is not yet available for large-scale use.[257]

Regarding so-called cross-usage of sensitive biometric data in European Court of Human Rights (ECtHR) case number 2017:T3872[258] regarding Finland, the European Court of Human Rights found that the rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union are not absolute rights. According to Article 52 (1) of the Charter, the exercise of these rights may be subject to limitations, when such limitations are provided for by law and respect the essence of the rights. Moreover, such limitations must be proportionate and meet the objectives recognized by the European Union and they must be necessary in order to protect the rights and freedoms of others. Similarly, according to Article 8 (2) of the ECHR, public authorities may not interfere with the right to private life except when such interference is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of

[255] Ministry of Interior, Civilian Intelligence Act to improve Finland's national security. Available at: https://intermin.fi/en/artikkeli/-/asset_publisher/siviilitiedustelulaki-parantaa-suomen-kansallista-turvallisuutta

[256] Finnish police, customs now able to use facial ID tech, but infrastructure not in place, published 06/06/2019. Online available: https://yle.fi/uutiset/osasto/news/finnish_police_customs_now_able_to_use_facial_id_tech_but_infrastructure_not_in_place/10818526

[257] Finnish police, customs now able to use facial ID tech, but infrastructure not in place. Op.cit.

[258] https://www.kho.fi/fi/index/paatoksia/muitapaatoksia/muupaatos/1502706198406.html

others.[259] The right of the police to use fingerprint data for purposes other than issuing and producing passports is strictly limited by law to situations where it is necessary to identify a victim of a natural disaster or other major disaster or catastrophe or a victim of crime or when a victim's identity cannot be verified by other means. In such cases fingerprints can be compared to fingerprints stored in [the passport] register. However, the data extracted from the register can only be used as long as the comparison is being carried out and must be erased immediately after the comparison has been completed. Therefore, and also in view of what has been presented above, it can be concluded that fingerprint data stored in the passport register meets the requirements set in Article 52 (1) [of the Charter] and Article 8 (2) of the ECHR and is also in accordance with the general requirements for limitations on constitutional rights, particularly the requirements of acceptability and proportionality.[260]

3.10. France

Police forces need an authorization by decree from the State Council (French "Conseil d'Etat"), and a favorable Opinion by the French Data Supervisory Authority (hereinafter the CNIL), before deploying facial recognition technology[261].

The following laws regarding offence proceedings, regulate the collection and use of facial images (a person's photographs):

1) **French Data Protection Act**[262]. In France, processing of biometric data on behalf of the State as part of its official powers as a public authority in criminal offence sphere is subject to provisions of this Act which includes **Title III: Provisions applicable to processing under Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of prevention and detection of criminal offenses, of investigations and prosecutions in the matter or of the execution of**

[259] Please see summary of this case in FRA Caselaw: Finland Supreme Administrative Court 3872/2017; 3736/3/15x v the Embassy of Finland in Switzerland. Online available: https://fra.europa.eu/en/caselaw-reference/finland-supreme-administrative-court-38722017-3736315 (15.11.2019).

[260] Please see summary of this case in FRA Caselaw: Finland Supreme Administrative Court 3872/2017; 3736/3/15x v the Embassy of Finland in Switzerland. Online available: https://fra.europa.eu/en/caselaw-reference/finland-supreme-administrative-court-38722017-3736315 (15.11.2019)

[261] Pursuant to articles 31, 32 of the French Data Protection Act, No 78-17 of January 6, 1978.

[262] French Data Protection Act No 78-17 of January 6, 1978, available at: https://www.cnil.fr/fr/la-loi-informatique-et-libertes, accessed 31/10/2019.

criminal sanctions, and of the free movement of such data, and repealing Council Framework Decision 2008/977 / JHA. These provisions largely mimic the GDPR and **Directive 2016/680 provisions.** In the context of criminal matter, the processing of personal data is admitted "*for the purpose of the prevention, investigation, detection, investigation and prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security, by any competent public authority or any other body or entity entrusted with the exercise of public authority and the exercise of the powers of public authority for the same purpose*"[263]. Thus, the scope of processing of facial images is only authorized "subject to the provision of appropriate safeguards for rights and freedoms of the data subject" and solely "to protect the vital interests of the data subject or of another individual; or when the processing relates to data which are manifestly made public by the data subject".[264]

The Gendarmerie in France has been using facial recognition technologies for criminal investigations but does not use live facial recognition technologies due to the absence of a legal basis to do so.[265]

2) Articles R. 40-23 to R. 40-34 of the French Criminal Procedure Code[266]. According to the aforementioned articles, "criminal records database" (hereinafter "Traitement des Antécédents Judiciaires" or "TAJ") allows to record photograph of the face from the front making it possible to use a facial recognition device. Non-real-time analysis of video surveillance images for facial recognition purposes by police and gendarmerie forces is currently limited to comparing images obtained during an investigation with the "criminal records database"– the only judicial police file that permits the use of facial recognition. **Article 78-3 of the French Criminal Procedure Code** determines that if an arrested person does not allow itself to be identified after authorization by the public prosecutor or the investigating judge it is possible to obtain fingerprints or photographs for establishing the identity.
French Data Protection Act (relevant articles are provided in the footnotes) and Articles R.40-23 to R.40-34 of the French Criminal Procedure Code are the only applicable legal texts regarding **automated facial recognition system in criminal proceedings in France.**

[263] Pursuant to Article 87 of the French Data Protection Act.
[264] Pursuant to Article 88 of the French Data Protection Act.
[265] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf - p. 12
[266] Articles R40-23 to R40-34 of the French Criminal Procedure Code:https://www.legifrance.gouv.fr/affichCode.do;jsessionid=6D202AD6A6FF4F3A1BFCBD391B18999D.tplgfr21s_2?idSectionTA=LEGISCTA000025818428&cidTexte=LEGITEXT000006071154&dateTexte=20120507, accessed 31/10/219.

Regarding detention of the persons the Penitentiary Act **(LOI n° 2009-1436 du 24 novembre 2009 pénitentiaire)**[267] regulates the collection and use of facial images.

Article 58-1 of this law states that the prison management administration may process personal data relating to CCTV of detention cells within penal establishments. This processing can only concern detention cells housing person placed in pre-trial detention, subject to a criminal detention warrant. They can only be implemented on an exceptional basis. No biometric device is coupled with these video surveillance treatments.

Regarding the use of identity documents, there is a facial recognition technology which used for external border crossings for passengers who have a biometric passport (the PARAFE system)[268]. Border control is carried out in an automated way for certain passengers. PARAFE system verifies identity by comparing a photo taken at the checkpoint with the image on their passport and the one stored in the chip.[269]

Also, the ALICEM digital identification system relies on the use of facial images for identification purposes. In May 2019 the Ministry of the Interior and Agence nationale des titres sécurisés (ANTS - the French National Agency for Secure Identity Documents), have put in place the ALICEM system (mobile-based certified online authentication)[270], making it possible for anyone with an Android telephone and a secure identity document (passport, residency permit) to have a secure digital identity. In an opinion published on 18 October 2018, the CNIL regretted the absence of an alternative to facial recognition and criticized the retention period for application access logs (6 years).[271]

For purposes of issuing identity cards and passports, Decree No 2016-1460 of 28 October 2016 authorizing the creation of a personal data processing relating to passports and national identity cards[272] allows processing of data for these purposes, including the digital image of the face. At the same time Article 2 of this decree specifically excludes use of automated means for identification from the image of

---

[267] **LOI n° 2009-1436 du 24 novembre 2009 pénitentiaire, entry into force 24/11/2009. Online available:** https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021312171&dateTexte=20191129, accessed 31/10/2019.

[268]The PARAFE system is provided for in Articles R.232-6 to R232-11 of the French Internal Security Code, available at: https://www.legifrance.gouv.fr/affichCode.do;jsessionid=8274EB9C7182C8EEF2DC7D4D8C2D1D24.tplgfr41s_1?idSectionTA=LEGISCTA000028287282&cidTexte=LEGITEXT000025503132&dateTexte=20200102

[269] http://www2.assemblee-nationale.fr/content/download/179314/1794787/version/2/file/Note+Reconnaissance+Faciale+-+EN.pdf p. 6

[270] Decree no. 2019-452 of 13 May 2019 authorizing the creation of an electronic identification method called "Authentification en ligne certifiée sur mobile" (Mobile-Based Certified Online Authentication: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038475477&dateTexte=20190722

[271] Opinion of the CNIL: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038475742 and http://www2.assemblee-nationale.fr/content/download/179314/1794787/version/2/file/Note+Reconnaissance+Faciale+-+EN.pdf p. 6

[272] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&categorieLien=id

the face. For management of cases in the fight against document fraud and identity theft on national identity cards and passports, personal data may be processed, however, Article 2 of the Order of 9 November 2011 establishing a processing of personal data relating to the fight against document fraud and identity theft[273] specifically excludes use of facial recognition on photographs.

According to laws the facial images are collected from the following group of persons:

1) The French Criminal Procedure Code (processing of „criminal record databases"):

- Persons in respect of whom there is serious or corroborating evidence during the preliminary investigation, the investigation of obvious offence or the investigation of letters rogatory which makes it likely that they may have participated, as perpetrators or accomplices, in the commission of a felony, misdemeanour or a fifth class offence or contravention;
- Victims of these offences;
- Persons being investigated or investigated for causes of death, serious injury or disappearance[274];

2) The Penitentiary Act - surveillance in detention house using CCTV: persons remanded in custody who are subject to a warrant for criminal detention[275];

3) Decree No 2016-1460 of 28 October 2016 - identity cards and passports: persons which require establishment, issuance, renewal of their identy cards or passports;

4) Order of 9 November 2011 - fight against document fraud and identity theft: persons suspected of being a usurper or fraudster;

5) Articles R.232-6 to R232-11 of the French Internal Security Code – PARAFE system: air, sea and rail travelers;

6) Decree no. 2019-452 of 13 May 2019 authorizing the creation of an electronic identification method called „ALICEM": French nationals holding a passport with an electronic component and foreign nationals holding a residence permit with an electronic component.

The purposes to use facial images according to the laws are the following:

[273] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024871453&dateTexte=20191129
[274] According to Article R40-45 of the French Criminal Procedure Code.
[275] According to Article 58-1 of the Penitentiary Act.

1) The French Criminal Procedure Code (processing of „criminal record databases“): to facilitate the detection of infringements of criminal law, the gathering of evidence of such infringements and the tracing of the perpetrators[276];

2) The Penitentiary Act - surveillance in detention house using CCTV: the purpose is to monitor the detention cells in which persons under judicial custody, subject to a solitary confinement measure, are assigned, whose escape or suicide could have a significant impact on public order in view of the circumstances giving rise to their incarceration and the impact of these circumstances on public opinion[277];

3) Decree No 2016-1460 of 28 October 2016 - identity cards and passports: in order to establish, issue, renew and invalidate national identity cards and passports;

4) Order of 9 November 2011 - fight against document fraud and identity theft: management of cases investigated as part of the fight against document fraud and identity theft on national identity cards and passports;

5) Articles R.232-6 to R232-11 of the French Internal Security Code – PARAFE system: improve and facilitate police checks at the external borders;
6) Decree no. 2019-452 of 13 May 2019 authorizing the creation of an electronic identification method called „ALICEM“: propose the delivery of an electronic identification means allowing them to identify themselves electronically and to authenticate themselves to public or private organizations, by means of a terminal electronic communications equipment equipped with a device allowing the reading without contact of the electronic component of these securities.

The facial images are stored in following databases:
1) The French Criminal Procedure Code (processing of „criminal record databases“): national police and gendarmerie services records.
2) The Penitentiary Act - surveillance in detention house using CCTV: prison management records.
3) Decree No 2016-1460 of 28 October 2016 - identity cards and passports: identity document databases implemented by the French Internal Ministry.

[276] According to Article R.40-24 of the French Criminal Procedure Code and Article 230-6 of the French Internal Security Code.
[277] According to Article 58-1 of the Penitentiary Act.

4) Order of 9 November 2011 - fight against document fraud and identity theft: General Secretary of the French Internal Ministry records.
5) Articles R.232-6 to R232-11 of the French Internal Security Code – PARAFE system: border and customs police officers records.
6) Decree no. 2019-452 of 13 May 2019 authorizing the creation of an electronic identification method called „ALICEM“: the French Internal Ministry records.

There is no specific provisions in French law allowing to use facial images which has been collected for other (civil purposes) in offence proceedings. However, Article 427 of the French Criminal Procedure Code allows to bring evidence in offence proceedings by any way, including video or image.

Cross-border cooperation in case of exchanging evidences or personal data is possible between the countries (government entities) according to the French Data protection Act Articles 87 to 114. Moreover, Articles R.40-24, R.40-28 and R.40-29 of the French Criminal procedure Code regarding “criminal record databases” provides that International judicial police cooperation agencies and foreign police services can be the recipients of this processing of personal data and exchange of personal data is admitted for international cooperation.

3.11. Germany

The laws regarding offence proceedings, which regulate the collection and use of facial images in Germany are:

1) German Code of criminal procedure (Strafprozessordnung)[278];

2) Federal Police Law (Gesetz über die Bundespolizei)[279];

[278] Strafprozessordnung, entry into force 7.04.1987, online available: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html, accessed 31/10/2019.
[279] Gesetz über die Bundespolizei, entry into force 19.10.1994, online available: https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html, accessed 31/10/2019.

3) Law on the Federal Criminal Police Office and the cooperation of the federal and state governments in criminal police matters, shortly Law on the Federal Criminal Police Office (Bundeskriminalamtgesetz)[280].

Taking photographs, including image recordings, is the measure of identification according to § 24 (3) of Federal Police Law. Federal Police Law states that in order to prevent criminal offenses, the collection of personal data is only permitted if facts justify the assumption that: a) the person wants to commit crimes within the meaning of § 12 (1) with considerable importance and the data are necessary to prevent such crimes or b) the person is connected or is connected to a person named in previous sentence in such a way that one can expect that the measure will prevent crime within the meaning previously listed and that this would otherwise be hopeless or considerably more difficult.[281] Data collection shall be open. According to § 21 (3) of Federal Police Law personal data shall be collected openly and from the person concerned. "Open" means in this situation that the data collection is not hidden, is recognizable as a police measure. They can be collected from other public or non-public bodies if it is not possible to collect the data from the person concerned or if it would jeopardize or significantly complicate the tasks of the Federal Police. A hidden data collection is permitted under § 21 (3) (phrase 3) when the federal police could not fulfill its tasks otherwise. They can be collected from other public or non-public bodies if the data cannot be collected from the person concerned or if it would jeopardize or significantly complicate the tasks of the Federal Police. Data collection, which should not be recognizable as a measure by the federal police, is only permitted if the fulfillment of the tasks incumbent on the federal police is significantly jeopardized or if it can be assumed that this corresponds to the overriding interest of the person concerned.

The Federal Police of Germany can use automatic image recording and recording devices according to § 27 of Federal Police Law in case of a) unauthorized border crossing or b) security threats at the border or there is dangers for the objects referred to in § 23 (1) no 4 of for persons or things located there to recognize[282]. In the case of automatic image recording in high risk public places (listed in § 23 (1) no 4), the use of such devices must be recognizable. If personal data are recorded in this way, these records must be destroyed after two days at the latest in the case described above in the point a) and after 30

[280] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, entry into force 1.06.2017, online available: http://www.gesetze-im-internet.de/bkag_2018/BJNR135410017.html, accessed 31/10/2019.
[281] § 21 (2) of Federal Police Law
[282] § 23 (1) no 4 lists following: the person is in an institution of the Federal Police, an installation or installation of the Federal Railways, an air transport installation or installation of a commercial airport, the official seat of a constitutional body or one Federal Ministry or at a border crossing point or in the immediate vicinity thereof

days at the latest in the case described in the point b) insofar as they are not needed to protection against current danger nor prosecution in a criminal offense or an administrative offense.

The German Federal Criminal Police Office may, insofar as this is necessary to fulfill its task as a central body in accordance with the law[283], collect personal data to supplement existing facts or otherwise for evaluation by means of information or inquiries from public or non-public bodies according to § 9 and § 12 (1) of Law on the Federal Criminal Police Office. According to § 2 (1) of the same legal act the Federal Criminal Police Office, as the central agency for the police information and news system and for the criminal police, supports the federal and state police in preventing and prosecuting crimes with cross-border, international or significant significance. The Article 12 (3) 1 (1) states that personal data obtained through the production of photographs or image recordings of a person through the hidden use of technical means in or from living rooms may not be further processed for law enforcement purposes.

The article 25 of Law on the Federal Criminal Police Offices regulates the data transmission in the domestic area, § 26 settles the data transmission to member states of the European Union and § 27 in the international area. The establishment of an automated procedure for the transmission of personal data by calling it up from the information system is only permitted to perform law enforcement tasks with the consent of the Federal Ministry of the Interior and the interior ministries and senate administrations of the federal states, in compliance with § 12 (2) to (4), provided that this form of data transmission is appropriate, taking into account the interests of the data subjects worthy of protection, due to the large number of transmissions or because of their particular urgency. The article 81 (2) applies accordingly.[284]

The Federal Criminal Police Office operates an information system[285] which fulfills the following basic functions according to § 13 (2) of Law of the Federal Criminal Police Offices: support in police investigations, support in tenders for and searches for people and things, support in the police information consolidation by clarification of clues and traces, carrying out comparisons of personal data, support in the creation of strategic analyzes and statistics. Article 14 regulates that during the storing in the information system, personal data must be identified (a) indication of the means of collecting the data, including whether the data was collected openly or concealed, b) specification of the category for persons for whom basic data has been collected, c) specifying the legal interests which needs the protection as well the offenses for the prosecution or prevention of which the data are collected, and d) indication of the body that collected it, unless the Federal Criminal Police Office collected the data). The

[283] In accordance with § 2 (2) number 1 and § 6 of Bundeskriminalamtsgesetz
[284] § 25 (7) of Bundeskriminalamtsgesetz
[285] § 13 of Bundeskriminalamtsgesetz

personal data that are not marked in accordance with the requirements listed before may not be further processed or transmitted until they have been labeled accordingly.[286]

The matter of the collection and use of facial images regarding detention of the persons is regulated by Act concerning the execution of prison sentences and measures of rehabilitation and prevention involving deprivation of liberty, shortly Prison Act (Strafvollzugsgesetz)[287]. According to § 86 (1) of Prison Act to secure imprisonment is allowed to take photographs as identification measure. Article 86 (2) notes that the identification data shall be included in the prisoner's personal file. They may also be kept in files pertaining to the criminal investigation; though this does not have or have little relevance in daily practice. The data collected in accordance with this article may only be processed and used for the named purposes: identification purpose to secure imprisonment[288], if this is necessary for purposes of search and apprehension of the prisoner who has escaped or is otherwise outside the institution without authorization[289] and for the prevention or prosecution of criminal offenses and for the prevention or prosecution of administrative offenses which jeopardize the security or order of the institution.

Persons who have been treated for identification purposes in accordance with § 86 (1) of Prison Act shall be entitled to demand that the identification data obtained be destroyed after their release from imprisonment with the exception of photographs and the description of physical characteristics.

According to § 86a (1) of Prison Act (irrespective of § 86) in order to maintain security and order in the institution, photographs of the prisoner may be taken and identified with the names of the prisoners and their date and place of birth. The photographs may only be taken with the knowledge of the prisoner. The photographs taken from the prisoner may only be used by prison staff if verification of the identity of prisoners is necessary in the context of carrying out their tasks and transmitted to the police execution authorities of the Federation and the Länder, where this is necessary to avert an immediate danger to significant legal interests within the institution, as well if this is necessary for purposes of search and apprehension of the prisoner who has escaped or is otherwise outside the institution without authorization.[290]

The legal regulations in Germany regarding issuance and use of identity documents regulating collection and use of facial images are: Act on Identity Cards and Electronic Identification

[286] § 14 (2) of Bundeskriminalamtsgesetz
[287] Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung, entry into force 16.03.1976, online available https://www.gesetze-im-internet.de/stvollzg/BJNR005810976.html, accessed 31/10/2019.
[288] § 86 (1) of Strafvollzugsgesetz
[289] § 87 (2) of Strafvollzugsgesetz
[290] § 86a, § 87 of Strafvollzugsgesetz

(Personalausweisgesetz)[291], Passport Act (Passgesetz)[292], Regulation implementing the Passport Act (Verordnung zur Durchführung des Passgesetzes)[293], Road Transport Act (Straßenverkehrsgesetz)[294], Regulation on permission to drive (Verordnung über die Zulassung von Personen zum Straßenverkehr, Fahrerlaubnis-Verordnung)[295]

The photograph of the passport holder is a standard specimen of the passport considering § 4 (1) of Passport Act. In accordance with Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, passports, official passports and diplomatic passports shall include an electronic storage medium which shall contain among other information facial image. The stored data shall be secured against unauthorized reading, alteration and deletion.[296] Following § 5 (4) the passport shall include a current photograph. During the passport issuance the passport authority may arrange to have passport applicants photographed and fingerprinted by the police if it would otherwise be impossible or extremely difficult to determine the applicant's identity. Once the applicant's identity has been confirmed, any documents collected for the purpose of determining such identity shall be destroyed. A record of the destruction shall be drawn up. As stated in § 6a (1) of Passport Act the data needed for the production of passports, in particular all data from passport applications, shall be sent from the passport authorities to the passport producer electronically. The data may also be transmitted via intermediary agencies. The bodies concerned shall take state-of-the-art measures to ensure data protection and data security, in particular to guarantee the confidentiality and integrity of the data, as well as the identification of the sending agency; when publicly accessible networks are used, state-of-the-art encryption methods shall be applied. Considering data protection provisions § 16 (2) rules that the passport application and issuance may not be used as a reason to store passport information and biometric identifiers anywhere other than with the responsible passport authorities.

The photographs are recorded in the passport register.[297] According to the § 22 (2) of Passport Act the passport authorities may transmit data in the passport register (including photographs) to other

[291] Personalausweisgesetz, entry into force 18.06.2009, online available: https://www.gesetze-im-internet.de/pauswg/BJNR134610009.html, accessed 31/10/2019.
[292] Passgesetz, entry into force 19.04.1986, online available: http://www.gesetze-im-internet.de/pa_g_1986/BJNR105370986.html, accessed 31/10/2019.
[293] Verordnung zur Durchführung des Passgesetzes, entry into force 19.10.2007, online available: http://www.gesetze-im-internet.de/passv_2007/BJNR238610007.html, accessed 31/10/2019.
[294] Straßenverkehrsgesetz, entry into force 5.03.2003, online available: https://www.gesetze-im-internet.de/stvg/BJNR004370909.html, accessed 31/10/2019.
[295] Verordnung über die Zulassung von Personen zum Straßenverkehr, Fahrerlaubnis-Verordnung, entry into force 13.12.2010, online available: https://www.gesetze-im-internet.de/fev_2010/BJNR198000010.html, accessed 31/10/2019.
[296] § 4 (3) of Passgesetz
[297] § 21 (2) of Passgesetz

authorities at their request under specific conditions: the requesting authority is authorized by law or statutory instrument to receive such data, the requesting authority would not be able to fulfil its assigned duties without knowledge of the data and the data cannot be obtained from the data subject without disproportionate effort, or the nature of the task for which the data are required means that the data cannot be collected in this way. Article 22 (4) allows to use the data from the passport register to correct data in the civil register and vice versa.

According to § 22a (2) of Passport Act when photographs are to be transmitted from the passport authorities to the agencies of public order in connection with the investigation of traffic offences, such photographs may be retrieved using an automated process. Such automated retrieval shall be permitted only when the passport authority is not reachable and waiting for longer would endanger the investigation. Law enforcement agencies at the level of districts and cities not associated with a district, to be designated by Land law, shall be responsible for retrieval. The retrieving authority shall be responsible for ensuring that the conditions of the law are met. Moreover, the federal police authorities, the police authorities of the Länder, as well as the intelligence agencies (the Federal Intelligence Service, the authorities for the Protection of the Constitution), the tax investigation authorities of the Länder and the authorities of the customs administration may retrieve photographs using an automated process to fulfill their tasks, as provided for in § 22a (2) (phrase 5). The authorities involved shall keep a record of all retrievals to enable their permissibility to be checked.

The photographs of identity cards holders are recorded in the Identity card register[298]. The Act on Identity cards and electronic identification contains similar regulations to § 22 and 22a of Passport Act.

The article 24 (2) of the Act on identity cards and electronic identification allows the identity card authorities to transmit data in the identity card register (including photographs) to other authorities under the same conditions as § 22 (2) of the Passport Act. The article 25 corresponds to § 22a of Passport Act. The article 25 (2) (phrase 4) of the Act on identity cards and electronic identification and § 22a (2) (phrase 5) of Passport Act, which allow police, intelligence and tax investigation agencies and authorities to retrieve photographs using an automated process, are both the result of amendments made by the Law to promote electronic means of identification[299]. The collection and use of facial images by state is regulated additionally by Police Laws of the Länder (for instance Allgemeines Gesetz zum Schutz der

[298] § 23 of Personalausweisgesetz

[299] Gesetz zur Förderung des elektronischen Identitätsnachweises, entry into force 7.07.2017, online available: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2310.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2310.pdf%27%5D__1578409684137, accessed 31/10/2019.

öffentlichen Sicherheit und Ordnung in Berlin [300]), Protection of the Constitution Act (Bundesverfassungsschutzgesetz)[301].

According to the Code of Criminal Procedure the facial images are collected from suspects and accused persons. Article 81b of Code of Criminal Procedure allows to take the photographs of the accused insofar as it is necessary for carrying out the criminal proceedings or for the purposes of the identification service also against his will. Towards the accused person also image recordings outside of living rooms are allowed without his knowledge according to § 100h (1) and (2) of Code of Criminal Procedure. The subject of the investigation shall be a criminal offence of considerable importance and researching the facts or determining the whereabouts of a suspect would otherwise be less promising or more difficult.

According to the § 161 the public prosecutor is authorized to request information from all authorities and to carry out any type of investigation himself or to have it carried out by the authorities and police officers, unless other statutory provisions regulate their powers in particular. The article 161 (2) states that insofar as the deletion of personal data is expressly ordered in this act, section 58 (3) of the Federal Data Protection Act does not apply. The article 161 (3) specifies if a measure is only permitted under this act if certain criminal offenses are suspected, the personal data obtained on the basis of a corresponding measure under other laws may only be used to investigate such criminal offenses without the consent of the persons affected by the measure, for evidence purposes in criminal proceedings. Such a measure should have been ordered to clarify this under this Act.

Photographing of the convicts is allowed under the Prison Act mainly in purpose of identification. Police Laws list suspect in the context of the prevention of criminal offences and everybody in the context of video surveillance. Collection of facial images from the persons who apply for an ID, passport, driving license is regulated by Act on Identity Cards and Electronic Identification, Passport Act and Regulation on permission to drive in order to issue the respective document.

As general rule deriving from § 98c of German Code of criminal procedure the personal data from criminal proceedings may, in order to investigate a crime or to determine a person´s whereabouts in connection with criminal proceedings, be automatically matched with other data stored for the purposes of criminal prosecution or execution of sentence, or in order to avert danger. Special rules under Federal law or under

[300] Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin, entry into force 9.08.2006, online available: http://gesetze.berlin.de/jportal/;jsessionid=68E784CA5AEF8FDB51E21B42DF30A4BA.jp26?quelle=jlink&query=ASOG+BE&psml=bsbeprod.psml&max=true&aiz=true#jlr-ASOGBE2006pP18

[301] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz), entry into force 20.12.1990, online available: https://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html, accessed 31/10/2019.

the corresponding *Land* law, shall remain unaffected. The article 48 of Law on the Federal Criminal Police Office allows the Federal Criminal Police Office to require public or non-public bodies to transmit personal data from certain groups of people for the purpose of automated comparison with other databases, insofar as this is in order to avert a threat to the existence or security of the Federation or a country or to the body, life or freedom of a person or property of significant value, the preservation of which is in the public interest, is required. The request for transmission must be limited to the name, address, day and place of birth and other characteristics to be determined in individual cases; it must not extend to personal data that are subject to professional or special official secrecy. Personal data not covered by requests for transmission may be transmitted if it is not possible to limit the data requested due to considerable technical difficulties or due to an inadequate expenditure of time or money; this data may not be used by the Federal Criminal Police Office. According to § 20 of Law of the Federal Criminal Police Office the Federal Ministry of the Interior, by means of an ordinance with the consent of the Federal Council, determines the details of the type and scope of the data that may be processed in accordance with § 16[302], 18[303] and 19[304].

According to Federal Data Protection Act (Bundesdatenschutzgesetz) [305] the data controller and processor shall take the necessary measures to ensure an adequate level of security. The Federal Office for Information Security shall adopt guidelines on data security. The Federal Office for Information Security (BSI) has adopted information security standards[306].

The article 49 of Federal Data Protection Act allows to process personal data for a purpose other than the one for which they were collected shall be permitted if the other purpose is one of the purposes listed in § 45 of the same act, the controller is authorized to process data for this purpose, and processing is necessary and proportionate to this purpose. The processing is allowed for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, as far the purpose of the processing the data is carrying out these tasks.[307] Personal data for another purpose not listed in § 45 shall be permitted if it is allowed by law.

[302] Data processing in the information system
[303] Data on convicts, accused, suspects and other causes
[304] Data on other persons
[305] Bundesdatenschutzgesetz, entry into force 30.06.2017, online available: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html, accessed 31/10/2019.
[306] BSI-Standard 100-1, Information Security Management Systems, online available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1.
[307] § 45 of Bundesdatenschutzgesetz

The article 78 (1) of Federal Data Protection Act regulates that if all other conditions applicable to data transfers are met, the transfer of personal data to bodies in third countries or to international organizations shall be permitted in case: a) the body or international organization is responsible for the purposes referred to in § 45, and b) the European Commission has adopted an adequacy decision pursuant to Article 36 (3) of Directive (EU) 2016/680.

3.12. Greece

The following legal acts regarding offence proceedings and detention of the persons, regulate the collection and use of facial images (person's photographs) in Greece:

1) Law 4624/2019[308], Personal Data Protection Authority, implementing measures for the Regulation (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data;
2) Law 2472/1997 **on the Protection of Individuals with regard to the Processing of Personal Data[309];**
3) Law 2776/1999[310], Reformation Code;
4) Presidential decree for the organization of Greek Police services no. 178/2014 (*ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ 'ΑΡΙΘΜ. 178 Οργανισμός Υπηρεσιών Ελληνικής Αστυνομίας*)[311]. Clarifying note: The binding force of the presidential decree is the same as a law. President has the relevant mandatory competence. According to the Article 30 (1) the Criminal Investigation Division has the mission of: crime monitoring, cooperation gathering and classifying all data elements; the perpetrators, the proposal legislative or

[308] Law no 4624/2019 of the Greek Republic, published 29.08.2019. Online available: http://tiny.cc/hkindz, accessed 31.10.2019.
[309] Law no 2472/1997 of Greek Republic on the Protection of Individuals with regard to the Processing of Personal Data, published 10/04/1997. Online available: http://tiny.cc/upindz, accessed 31.10.2019.
[310] Law no 2776/1999 of Greek Republic, published 24/12/1999. Online available: http://www.et.gr/index.php/nomoi-proedrika-diatagmata, accessed 31.10.2019.
[311] ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ 'ΑΡΙΘΜ. 178 Οργανισμός Υπηρεσιών Ελληνικής Αστυνομίας, published 31/12/2014. Online available: https://www.e-nomothesia.gr/kat-astynomikos-astynomia/idrysi-leitourgia-uperesion/pd-178-2014.html, accessed 31/10/2019.

other appropriate measures prosecuting crimes and coordinating action all regional forensic services of the country.

Article 24 states: A) Department of Audiovisual Material, Photography and Procedures has the fallowing powers: (aa) monitors the activity, indications and actions of criminals and classifies them into specific categories, depending on the type of crimes, their method of detection and the physical characteristic or other characteristics of the perpetrators whose photos are kept in special collections (Modus Operandi); (bb) maintains a digital archive of photographs and data of the criminals involved and professionals through the Automatic Archive - Search System Photo (I.S.I.S.), creates sketches of suspects or look for faces and make photo comparisons; (cc) examines and processes electronic, photographic and video material from crime scenes or other police-related incidents and extracts improved images for use by judicial or other prosecuting authorities; (dd) uses all modern technological means to accomplish the mission more effectively and, at the request of the Public Authorities, specific technical reports on the technical parameters photo counters, video optics and electronic - digital icons.

B) Responsibilities of Video and Image Testing Laboratory: 1) examines and processes photographic and video material related to criminal acts or other police events for analysis and interpretation and extracts improved images for use by judicial or other law enforcement authorities; 2) examines analog or digital video recording devices CCTV from crime scenes or other police-related incidents, for reading, extracting and copying controversial video material, for forensic examination and investigation; 3) controls authenticity of video and photographic material; 4) examines video material which contains audio-visual compatibility testing, synchronization and authentication; 5) performs comparative photo examinations of persons, persons and objects between an unknown material sample and a sample disciplines of known material to identify or differentiate them; 6) perform searches of a pictured persons of unknown identities in the photographer's archive and professionally in-tagged individuals, to discover the data his identity.

List of laws about issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Greece, are as follows:

1) Ministerial Decision 3021/22/2005[312] for the issuance of passports;

2) Ministerial Decision 3021/19/5/2005[313] for the issuance of IDs;

[312] Ministerial Decision 3021/22/2005, published 06.07.2005. Online availble: http://www.passport.gov.gr/en/downloads/nomothetiko-plaisio/11.html, accessed 31.10.2019.

[313] Ministerial Decision no. 3021/ published 18/10/2005. Online available: https://www.e-nomothesia.gr/kat-deltia-tautotetos/kya-3021-19-53-2005.html, accessed 31.10.2019

3) Presidential Decree 51/2012[314] and Ministerial Decision 50984/7947/2013[315] for the issuance of driving licenses.

According to Presidential decree no. 178/2014 the facial images/photographs are collected from the following groups of persons: suspects, detainees, criminals. Photographs are collected also from passport / ID-cards / driving license holders.

The main purposes to use facial images/photographs according to Presidential decree no. 178/2014 and other above-mentioned legal acts are: investigate a crime, protection of the wider public and facilitation in the prosecution of relevant offences and identification.

The photographs of criminals are stored in the Greek Police Search National Database.

According to Article 24 of the Law 4624/2019, personal data, including facial images, which has been collected for other (civil) purposes may be processed when it is necessary for the prosecution of offenses and criminal proceedings.

According to Article 2 § b of Law 2472/1997, data concerning criminal prosecution and convictions are sensitive personal data. Those data may be published with the order of the competent Public Prosecutor, only when the case is pending at the Court of Appeal and only for a closed number of types of offenses. Such publication aims to protect society, minors, and vulnerable groups. Article 3 § 2 of the same law sets the scope of this Law.

Article 23 of Law 2776/1999 regulates the procedure of the collection of personal data during their detention. Their most recent pictures are attached on the relevant procedural documents and kept in their personal files.

According to Presidential decree no. 178/2014 and European Union regulations the Cross-border cooperation in case of exchanging information related to offence proceedings is possible between the countries (government entities).

[314] Ministerial Decree no. 51/2012, published 27/4/2012. Online available: https://www.e-nomothesia.gr/kat-aytokinita/adeies-odegeses/pd-51-2012.html, accessed 31.10.2019.
[315] Ministerial Decision no. 50984/7947/2013, published 02.12.2003. Online available: https://www.e-nomothesia.gr/kat-aytokinita/adeies-odegeses/ya-a3-oik-50984-7947-2013.html, accessed 31.10.2019.

Presidential decree no. 178/2014 Article 27 stipulates that information and data means: a) any information or data held by law enforcement authorities; b) any kind of information or data held by public authorities or by private individuals and is accessible to law enforcement authorities.

3.13. Hungary

The following laws regarding offence proceedings and the detention of persons regulate the collection and use of facial images (person's photographs) in Hungary:

1) Criminal Code (*2012. évi C. törvény a büntető törvénykönyvről*)[316]
According to section 3 point 2 of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("Information Act") and section 4 point 1 of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), facial images are considered personal data.

Accordingly, the following sections of the Criminal Code regulate crimes that mainly concern personal data and potentially facial images: Section 219 (misuse of personal data), Section 265 (criminal offences with classified information), Section 307 (unauthorised covert information gathering or illegal use of covert means), Section 422 (illicit access to data), Section 423 (breach of information system or data), Section 424 (compromising or defrauding the integrity of the computer protection system or device).

The following sections of the Criminal Code regulate crimes which potentially concern facial images: Sections 342-343 (forgery of administrative documents), Section 344 (forgery of secure identification documents), Section 345 (use of a forged private document), Section 346 (criminal offences with authentic instruments), Section 373 (fraud), Sections 384-387 (crimes regarding intellectual property).

[316] 2012. évi C. törvény a büntető törvénykönyvről, entry into force 01.07.2013. Online available: https://net.jogtar.hu/jogszabaly?docid=A1200100.TV, accessed 31.10.2019.

2) Act No. II of 2012 on misdemeanors, misdemeanour procedures and the register of misdemeanours (*2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről*)[317]

3) Act No. XC of 2017 on Criminal Proceedings (*2017. évi XC. Törvény a büntetőeljárásról*)[318] According to section 269 of the Criminal Proceedings Act, the prosecutor, the investigation authority and the crime prevention and investigation and counter terrorist bodies of the police are entitled to request facial image analysis.

4) CCXL of 2013 Criminal Execution Act (*2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról*)[319] Section 76 (1) f), j), l), and r) of the Act set out that the court, the prosecutor and the entities responsible for the execution of sentences (e.g. prisons), the reformatory institute and probation agencies are entitled to process the facial images of prisoners or persons in detention under other legal bases.
According to Section 89 (4) of the Criminal Execution Act, prisons are entitled to take facial images of prisoners for identification purposes and send them to the register of facial image profiles for facial image analysis, and Section 89 (6) c) provides that prisons are entitled to obtain the respective facial image from the register of aliens if there are doubts regarding the identity of the prisoner.
According to 347 (2) b) of the Criminal Execution Act, the reformatory institute is entitled to take facial images of underaged persons at the time of their admission to the reformatory institution in order to check their entrance into and exit from the institution.

5) IM Decree No. 16/2014 (XII.19.) on the detailed rules of the execution of imprisonment, detention, arrest and the detention replacing fine (*16/2014. (XII. 19.) IM rendelet a szabadságvesztés, az elzárás, az előzetes letartóztatás és a rendbírság helyébe lépő elzárás végrehajtásának részletes szabályairól*)[320]. According to Section 12 institutions responsible for the execution of penal sentences (e.g. prisons) are obliged to check the identity of persons entering the respective penal facility in order to verify their

[317] 2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről, entry into force 15.04.2012. Online available: https://net.jogtar.hu/jogszabaly?docid=A1200002.TV, accessed 31.10.2019.
[318] 2017. évi XC. Törvény a büntetőeljárásról, entry into force: 01.07.2018. Online available: https://net.jogtar.hu/jogszabaly?docid=A1700090.TV, accessed 31.10.2019.
[319] 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról, entry into force 01.01.2015. Online available: https://net.jogtar.hu/jogszabaly?docid=A1300240.TV#lbj0id899a, accessed 31.10.2019.
[320] 16/2014. (XII. 19.) IM rendelet a szabadságvesztés, az elzárás, az előzetes letartóztatás és a rendbírság helyébe lépő elzárás végrehajtásának részletes szabályairól, published 2014. Online available: https://net.jogtar.hu/jogszabaly?docid=a1400016.im, accessed 31.10.2019.

identity, in particular, the facial image of the person who enters the facility shall be compared to those of the convicted person. Section 67 stipulates that the penal institution is obliged to issue certificate to the prisoner (i) who goes on a temporary leave or short period leave or (ii) whose sentence is suspended (in Hungarian: "*félbeszakadás*"). The certificate contains, inter alia, the personal data and the facial image of the person concerned.

List of legal acts and regulations on the issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Hungary:

1) Address Registry Act (*1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról*)[321]
2) Identity Decree (*414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól*)[322]
3) Travelling Act (*1998. évi XII. törvény a külföldre utazásról*)[323] – it sets out the framework rules regarding the issuance of passports
4) Travelling Decree (*101/1998. (V. 22.) Korm. rendelet a külföldre utazásról szóló 1998. évi XII. törvény végrehajtásáról*)[324] – it sets out the detailed rules of the issuance of and application for a passport
5) Transport Decree (*326/2011. (XII. 28.) Korm. rendelet a közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról*)[325] – it sets out the detailed rules of the issuance of driving license
6) Warranted Persons Act (*2013. évi LXXXVIII. törvény a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról*)[326]

In addition to the abovementioned legal regulations, the following legal acts regulate the collection and use of facial images:

[321] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról, published 1992. Online available: https://net.jogtar.hu/jogszabaly?docid=99200066.TV, accessed 31.10.2019.
[322] 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól, published 2015. Online available: https://net.jogtar.hu/jogszabaly?docid=A1500414.KOR, accessed 31.10.2019.
[323] 1998. évi XII. törvény a külföldre utazásról, published 1998. Online available: https://net.jogtar.hu/jogszabaly?docid=99800012.TV, accessed 31.10.2019.
[324] 101/1998. (V. 22.) Korm. rendelet a külföldre utazásról szóló 1998. évi XII. törvény végrehajtásáról, published 1998. Online available: https://net.jogtar.hu/jogszabaly?docid=99800101.KOR, accessed 31.10.2019.
[325] 326/2011. (XII. 28.) Korm. rendelet a közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról, entry into force 01.01.2012. Online available: https://net.jogtar.hu/jogszabaly?docid=A1100326.KOR, accessed 31.10.2019.
[326] 2013. évi LXXXVIII. törvény a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról, published 2013. Online available: https://net.jogtar.hu/jogszabaly?docid=A1300088.TV, accessed 31.10.2019.

1) Analyzing Act (*2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről*)[327]. The Analyzing Act sets out the rules applicable for the facial images analyzation/profile register and the facial image analyzing system.

Section 1 stipulates the meanings of important terms, for instance:

'***Facial image***' – a photograph of a citizen's face taken or processed using an IT device capable of forming a facial profile;

'***Facial analysis system***' – an IT application capable of generating and comparing facial images, which facilitates identification;

'***Facial image register':*** the official record of the facial images provided by the body (designated by the Government) responsible for communicating information, including its associated technical switching number and metadata. According to Section 3 the purposes to keep the facial images register are for instance:

a) **The prevention, deterrence, detection and cessation of criminal offenses and the apprehension and prosecution of perpetrators**;

b) **The identification of the convicted and other persons held in custody at the time of admission to the prison**;

c) Identification of the applicant in administrative proceedings for the issue of an identity card;

d) **Assisting foreign authorities in the identification of the person subject to proceedings for the purpose of preventing, detecting and prosecuting criminal offenses**;

e) Establishing the identity of the persons applying to cross the border or the persons covered by the Asylum Law;

f) Establishing the applicant's identity during the procedure for acquiring Hungarian citizenship;

g) Support for national security services' national security audits, as well as for statutory intelligence, national security defense and response, intelligence, national security, industrial security, internal security and crime prevention, and operational protection of facilities and etc. The prosecuting authority, the prosecutor's office, the court, the police, the prison are entitled to use the facial recognition in order to fulfill their tasks (a detailed list of qualified entities is given in Section 9).

2) Act No. XLVII of 2009 on the criminal registry system, the registry of judgments against Hungarian citizens passed by the courts of Member States of the European Union and the **registry of criminal and police biometric data** (*2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió*

[327] 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről, published 2015. Online available: https://net.jogtar.hu/jogszabaly?docid=A1500188.TV, accessed 31.10.2019.

tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról)[328]
According to this Act, facial images are collected for the purposes of identifying whether a person is under criminal procedure.

3) Transport Registry Act (*1999. évi LXXXIV. törvény a közúti közlekedési nyilvántartásról*)[329] – it sets out the rules in respect of the information regarding transport documents (e.g. driving licenses)

According to Hungarian laws, facial images are collected from the following groups of persons:
1) Based on the Criminal Execution Act – facial images of prisoners or persons in detention under another legal title
2) Based on the Address Registry Act – facial images of each Hungarian citizen above the age of 14 are collected in relation to the issuance of their identity card
3) Based on the Transport Registry Act – facial images of persons obtaining transportation documents e.g. driving license
4) Based on the Travelling Act and Travelling Decree – facial images of persons obtaining travel documents (e.g. passports)

The purpose of using facial images depends on the legal basis as follows:
1) to prevent and investigate crimes (based on the Criminal Code, Criminal Proceedings Act)
2) to prevent and investigate crimes, identify persons in detention and warranted persons (based on the Analysing Act)
3) for identification (based on the Address Registry Act, Transport Registry Act)

According to the abovementioned legal acts, facial images are stored in the following databases:
1) Register of personal data and addresses (based on the Address Registry Act).
2) Register of driving licenses (based on the Transport Registry Act).
3) **Register of facial analysis (based on the Analysing Act).**

[328] 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, entry into force 30.06.2009. Online available: https://net.jogtar.hu/jogszabaly?docid=A0900047.TV, accessed 31/10/2019.
[329] 1999. évi LXXXIV. törvény a közúti közlekedési nyilvántartásról, published 1999. Online available: https://net.jogtar.hu/jogszabaly?docid=99900084.TV, accessed 31.10.2019.

4) Register of personal data and photographs, Criminal registers (based on Act No. XLVII of 2009 on the criminal registry system, the registry of judgments against Hungarian citizens passed by the courts of Member States of the European Union and the registry of criminal and police biometric data).
5) Register of warranted persons (based on Warranted Persons Act).

Hungarian laws allow the use of data, including facial images, which have been collected for other (civil) purposes to be used in offence proceedings. As set out in Section 167 (1) of the Criminal Proceedings Act, any evidence which the laws define as such may be used and any evidencing measures may be applied in a criminal procedure. According to section 167 (2) of the Criminal Proceedings Act, any physical item (including documents) may be used as evidence in a criminal procedure, provided that the physical item was obtained or prepared by an authority while performing its tasks defined in the applicable laws before or during the respective criminal procedure.

Pursuant to section 167 (5) of the Criminal Proceedings Act, information which the court or the prosecutor or investigation authority or the authority which obtained the information or prepared the physical item while performing its tasks as an authority obtained by committing a crime or obtained through any other restricted method or obtained by materially infringing the criminal procedural rights of the respective parties of the criminal procedure. According to section 214 of the Criminal Proceedings Act, certain authorities are authorised to apply certain concealed tools for gathering information without the concerned person's knowledge, which restricts the fundamental rights for inviolability of private premises, confidentiality of correspondence and data privacy. In line with section 214 (3) of the Criminal Proceedings Act, certain concealed tools may be applied without the approval of the court or the prosecution authority; the approval of the court or the prosecution authority are necessary for the application of other concealed tools.

Pursuant to Section 214 (5) of the Criminal Proceedings Act, concealed tools may be applied during the criminal procedure if:
1) there are reasonable grounds to believe that the information to be obtained by the concealed tool is inevitable for achieving the purpose of the criminal procedure and cannot be obtained otherwise;
2) the application of the concealed tool does not restrict the concerned person's or another person's fundamental right which is disproportionate compared to achieving the purpose of the law enforcement agency;
3) it is likely that information or evidence related to a crime can be obtained by the application of the concealed tool.

Sections 215-255 of the Criminal Proceedings Act regulate the detailed provisions regarding the application of concealed tools. Facial images obtained during the criminal procedure by the above methods are collected and used for evidencing purposes.

Cross-border cooperation in the case of exchanging evidence is possible between countries (government entities). **The authorities of other countries are not entitled to request information directly from databases collecting facial images.** However, the authorities of other countries are entitled to issue a request for criminal assistance in line with the provisions of Act XXXVIII on the international criminal legal assistance (*1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről*)[330] or, if the other country concerned is an EU member state, in line with the relevant EU legislation.

3.14. Ireland

The law of Ireland consists of constitutional, statute and common law. The highest law in the State is the Constitution of Ireland, from which all other law derives its authority. The Republic has a common-law legal system with a written constitution that provides for a parliamentary democracy[331].

In accordance with Article 6a of Protocol No. 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union (the TEU) and to the Treaty on the Functioning of the European Union (the TFEU), Ireland is not bound by the rules laid down in Directive (EU) 2016/680 which relate to the processing of personal data by Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 of the TFEU.[332]

The following laws regarding offence proceedings, regulate the collection and use of facial images (a person's photographs):

[330] 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről, published 1996. Online available: https://net.jogtar.hu/jogszabaly?docid=99600038.TV, accessed 31.10.2019.
[331] https://en.wikipedia.org/wiki/Law_of_the_Republic_of_Ireland
[332] Recital 99 of Directive (EU) 2016/680.

1) Data Protection Act[333]. According to Part 5 (Processing of Personal Data for Law Enforcement Purposes) Section 69 of this Act, **'biometric data' means personal data resulting from specific technical processing** ('processing' includes by automated means) relating to the physical, physiological or behavioral characteristics of an individual that allow or confirm the unique identification of the individual, **including facial images** or dactyloscopic data;

2) GARDA SÍOCHÁNA (Ireland's National Police and Security Service) ACT[334]. According to Section 98 of this Act, police officers can search a person and take their **photographs**, fingerprints and palmprints. Section 38 of this Act (Security in public places): (1) provides that the Garda Commissioner may authorise the installation and operation of **CCTV** for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences. (14) **'CCTV' means any fixed and permanent system employing optical devices for recording visual images of events occurring in public places**;

3) Criminal Justice (Forensic Evidence and DNA Database System) Act[335]. According to Section 100 a member of the Garda Síochána may use such force as is reasonably considered necessary to take the **photograph** or fingerprints and palm prints from detained persons if these persons refuse to allow his or her **photograph** or fingerprints and palm prints to be taken pursuant to Criminal Justice Act. Destruction and retention of fingerprints, palm prints and **photographs** are regulated in Section 103.

4) Europol Act[336] - regulates the use and processing of personal data. Facial recognition is not explicitly mentioned, but according to Section 1 personal data has the meaning it has in Part 5 of the Data Protection Act 2018 and it contains facial images.

The legal act regarding the detention of persons, which regulates the collection and use of facial images in Ireland, is the Prison Rules[337]. According to Section 10:

[333] Data Protection Act no 7 of 2018. Online available: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/pdf, accessed 31/10/2019.
[334] GARDA SÍOCHÁNA ACT no 20 of 2005. Online available: http://www.irishstatutebook.ie/eli/2005/act/20/enacted/en/pdf, accessed 31/10/2019.
[335] Criminal Justice (Forensic Evidence and DNA Database System) Act no 11 of 2014. Online available: http://www.irishstatutebook.ie/eli/2014/act/11/enacted/en/pdf, accessed 31.10.2019.
[336] Europol Act no 53 of 2012. Online available: http://www.irishstatutebook.ie/eli/2012/act/53/enacted/en/pdf, accessed 31.10.2019.
[337] Prison Rules 2007. Online available: http://www.irishstatutebook.ie/eli/2007/si/252/made/en, accessed 31/10/2019.

1) the Governor of a prison may take and record, or cause to be taken and recorded, measurements, **photographs**, fingerprints and palm prints **of a prisoner at any time during the period of his or her imprisonment**;

2) The Governor of a prison may provide or cause to be provided to the Garda Síochána, the measurements, **photographs**, fingerprints or palm prints **of a prisoner** upon lawful application by a member of the Garda Síochána.

List of laws on the issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Ireland:

1) Passports Act[338]

2) Social Welfare and Pensions Act[339]

3) Employment Permits Regulations[340]

4) Road Traffic Regulations[341]

In addition to the abovementioned acts, the Immigration Act[342] regulates the collection and use of facial images.

According to legal acts, facial images/photographs are collected from the following groups of persons:

1) GARDA SÍOCHÁNA ACT – suspected;

2) Criminal Justice (Forensic Evidence and DNA Database System) Act – detained, arrested, convicted;

3) Prison Rules – prisoners.

The main purposes of using personal data, including facial images, according to the Data Protection Act in the meaning of law enforcement are the following: prevention, investigation, detection or prosecution of criminal offences, including safeguarding against and the prevention of threats to public security or the execution of criminal penalties.

[338] Passports Act no 4 of 2008. Online available: http://www.irishstatutebook.ie/eli/2008/act/4/enacted/en/pdf, accessed 31.10.2019.

[339] Social Welfare and Pensions Act no 8 of 2007. Online available: http://www.irishstatutebook.ie/eli/2007/act/8/enacted/en/pdf, accessed 31.10.2019.

[340] Employment Permits Regulations no 95 of 2017. Online available: http://www.irishstatutebook.ie/eli/2017/si/95/made/en/pdf, accessed 31.10.2019.

[341] Road Traffic Regulations no 326 of 2014. Online available: http://www.irishstatutebook.ie/eli/2014/si/326/made/en/pdf, accessed 31.10.2019.

[342] Immigration Act no 1 of 2004. Online available: http://www.irishstatutebook.ie/eli/2004/act/1/enacted/en/pdf, accessed 31.10.2019.

There is no information available to us regarding the exact national database in which the facial images are stored and processed.

In some cases, the law simply states that the responsible authority must store the data but does not provide an exact location. According to the Europol Act, the Irish police has access to the Europol Information System.

According to Criminal Records (Exchange of Information) Act 2019[343] Section 1 "Criminal Records Database" means the database maintained by the Garda Síochána that contains a record of convictions. Section 6 stipulates that information from the Criminal Records Database in relation to a person is required — (a) for the purposes of criminal proceedings against the person in the State. This information may contain fingerprints, but facial images or photographs are not mentioned.

Information, regarding the laws in Ireland which allow to use data, including facial images, which has been collected for other (meaning civil) purposes to be used in offence proceedings, is not available to us.

Cross-border cooperation in the case of exchanging evidence and personal data is possible between countries (government entities) according to the Garda Siochana Act (Section 28) and the Europol Act.

3.15. Italy

The following legal acts regarding offence proceedings and detention of the persons, regulate the collection and use of facial images (person's photographs) in Italy:

1) Law of Public Security (*Leggi di pubblica sicurezza*)[344]. Article 4 states that the public security authority has the power to order that dangerous or suspicious people and those who are unable or unwilling refuse to prove their identity **are subject to** identification surveys (such as includes descriptive, photographic, fingerprinting and anthropometric).

[343] Criminal Records (Exchange of Information) Act 2019. Online available: http://www.irishstatutebook.ie/eli/2019/act/51/enacted/en/pdf, accessed 31/10/2019.

[344] Leggi di pubblica sicurezza, entry into force 11/07/1931. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1931-06-18;773!vig=, accessed 31/10/2019.

2) Implementing regulation of the public security laws (*Regolamento per l'esecuzione delle leggi di pubblica sicurezza*)[345]. According to Article 7 The warning signs for dangerous or suspicious people and for those who are unable or unwilling to try their own identity, according to art. 4 (The local public security authority exercises within the scope of the district of the municipality, the attributions that the laws refer to its competence.) of the law, are descriptive, **photographic**, dactyloscopic or anthropometric;

3) Criminal Procedure Code (*Codice di procedura penale*)[346]. According to Article 349 fingerprints, **photographic** and anthropometric **examinations may be used in criminal investigations.**; Article 114 § 6 states that Publication of the particulars and image of minors who are witnesses, persons who have been injured or injured by the crime is prohibited up to the age of majority. The court for minors, in the sole interest of the minor, or the minor who has reached the age of 16, may permit publication. It is also prohibited to publish elements which, even indirectly, can nevertheless lead to the identification of these minors. According to § 6-bis of the same Article the publication of the image as a private person of the personal freedom is prohibited while the same is subjected to the use of handcuffs to the wrists or other means of physical coercion, unless the person allows it.

4) Law Decree no 59 Criminal and procedural rules for the prevention and repression of serious crimes (DECRETO-LEGGE n. 59 Norme penali e processuali per la prevenzione e la repressione di gravi reati)[347]. Article 7: **Police may keep persons for identification, but not longer than 24 hours;**

These four above mentioned legal acts regulate the processing of biometric data also obtainable from the facial image, carried out by the police forces for the purpose of prevention, investigation, detection and prosecution of crimes or execution of criminal sanctions[348].

5) Ministry of the Interior decree no 33 (*Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196.*)[349]. This Decree

[345] Regolamento per l'esecuzione delle leggi di pubblica sicurezza, entry into force 11/07/1940. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1940-05-06;635, accessed 31/10/2019.

[346] Codice di procedura penale, entry into force 24/10/1989. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447, accessed 31/10/2019.

[347] DECRETO-LEGGE n. 59 Norme penali e processuali per la prevenzione e la repressione di gravi reati, 21/03/1978. Online available: https://www.gazzettaufficiale.it/eli/id/1978/03/22/078U0059/sg, accessed 31/10/2019.

[348] Opinion of the Italian Data Protection Authority **on Automatic system for searching the identity of a face, 26/07/2018. Online available:** https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256, accessed 02/01/2020.

[349] Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196, 24/05/2017. Online available: https://www.gazzettaufficiale.it/eli/gu/2017/06/24/145/so/33/sg/pdf, accessed 31/10/2019.

sets out the rules for the police service's video photography system. **A.F.I.S. (Automated Fingerprint Identification System) - S.S.A. (Subsystem of the investigative activities)** allows to search the archive of photos reported through the manual work of an operator, who must enter personal information, characteristics and marks in the fields on the query mask, for example, hair color, eyes, tattoos), in order to identify the presence of the subject in the AFIS archive;

6) Criminal Code (*Codice Penale*)[350] – Article 651 states that any person who, on request of a public official, according to art. 357, 366 criminal code in the performance of his duties, refuses to give any indication of his personal identity, state or other personal qualities, is punished by arrest for up to one month or with a fine of up to EUR 206;

7) Deontological rules concerning the processing of personal data carried out to carry out defensive investigations or to assert or defend a right published in court pursuant to art. 20, par. 4 Legislative Decree, n. 101 August 2018 – December 19, 2018 (*Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069653]*)[351] – These rules establish the general principles applicable on the utilization and destruction of data reported on devices or media, especially electronic (including audio/video recordings). The processing take place also in case before proceeding are pending. The data must be strictly relevant for the exercise of the right of defense, in accordance with the principles of lawfulness, proportionality and data minimization with respect to defensive purposes.

List of legal regulations about issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Italy, are the following:

1) The Italian Passport Law (*Legge 21 novembre 1967, n. 1185 (1). Norme sui passaporti (1/a) (1/circ))*[352];

2) Identity Card Law - there is no correct reference to this law.

3) Minister of infrastructure and transport department and transport, navigation, general affairs and staff Directorate-General for Motor Vehicles Division 5 protocol No. 23176/8.3[353] (***Fotografie da apporre sulla patente di guida***).

---

[350] Codice Penale, entry into force 01/07/1931. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1930-10-19;1398, accessed 31/10/2019.

[351] Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069653], 19/12/2018. Online available: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069653, accessed 02/01/2020.

[352] Legge 21 novembre 1967, n. 1185 (1). Norme sui passaporti (1/a) (1/circ)), 21/11/1967. Online available: https://www.esteri.it/mae/doc/l1185_1967.pdf, accessed 31/10/2019.

[353] **Fotografie da apporre sulla patente di guida, 20/10/2016. Online available:** http://www.patente.it/normativa/circolare-20-10-2016-n-23176-foto-per-patente?idc=3366, accessed 31/10/2019.

According to Italian laws the facial images are collected from the following groups of persons:

1) Criminal Procedure Code – suspects, defendants, victims, accused, convicts;

2) Criminal Code – convicts;

3) The Identity Card and Passport Law - Italian Citizens who apply obtaining identity card and / or passport;

4) Minister of infrastructure and transport department and transport, navigation, general affairs and staff Directorate-General for Motor Vehicles Division 5 protocol No. 23176/8.3 - a person applying for a driving license and having his / her permanent residence in Italy;

5) Video surveillance Laws (according article 234 Criminal Procedure Code which states that the acquisition of writings or other documents representing facts, persons or things by photography, film, phonography or any other means is permitted, and other special laws, for example, related to employees proceeding set out by art. 4 Law no. 300/1970) - a natural person captured by video cameras, who can be identified by the image captured in the video.

The main purposes to use facial images depend on legal basis as follows:

1) Criminal offense investigation (Criminal Procedure Code, Criminal Code);

2) to ensure public order, public and property security and to implement misconduct prevention (Video surveillance Laws such as article 234 Criminal Procedure Code and art. 4 Law no. 300/1970.

Facial images are stored in AFIS-SSA System (Ministry of the Interior decree no 33) and SARI Enterprise System [354] – for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the enforcement of criminal sanctions.

Deontological rules concerning the processing of personal data **allow to use data, including facial images, which has been collected for other (civil) purposes to be used in offence proceedings.**

Cross-border cooperation in case of exchanging facial images (photographs) **is possible** between the countries (government entities).

For example, in Italy, the Interministerial Decree No. 4516/495 of 6 October 2011 states that the VIS (VISA INFORMATION SYSTEM) may only be accessed by the duly authorized staff for purposes related to the issue, extension, annulment, revocation or refusal of entry visas in the territory of the States that apply the Schengen Convention.

[354] Opinion of the Italian Data Protection Authority. Op.cit.

3.16. Latvia

According to Article 25(2) of the Personal Data Processing Law, biometric data processed for purposes of unique identification of a person shall be considered as processing of special category of data and may be processed under legal grounds established in Article 9(2) of the GDPR or if the data processing is determined in a legal act as provided by Article 9(4) of the GDPR. In general, main relevant laws regarding offence proceedings, which regulate the collection and use of facial images in Latvia, are the Biometric Data Processing System Law[355] and the Criminal Procedure Law[356]. Personal Data Processing Law nor any other special laws do not directly use and define the term "facial recognition". Thus, this notion shall be interpreted within the existing definitions of the legal acts.

The purpose of the Biometric Data Processing System Law is to ensure the establishment of a unified biometric data processing system to make it possible to determine identity of natural persons, and also to prevent the use of another person's identity (Section 2 of the Biometric Data Processing System Law). In accordance with Section 1 subparagraph 1) and 2) of this law *biometric data processing* means any activities carried out with biometric data, including data acquisition, registration, storage, sorting, modification, use, comparison, transfer, transmission, disclosure, blocking or deletion of the data, but *biometric data* is a set of physical properties of a natural person, including digitalised picture of a face, finger (palm) trails or prints.

In accordance with Section 127 (1) and (3) of the Criminal Procedure Law *an evidence* in criminal proceedings is any information acquired in accordance with the procedures provided for in the law, and fixed in a specific procedural form, regarding facts that persons involved in the criminal proceedings use, in the framework of the competence thereof, in order to justify the existence or non-existence of conditions included in an object of evidence. Information regarding facts acquired in operational activities measures, and information that has been recorded with the assistance of technical means, shall be used as evidence only if it is possible to examine such information in accordance with the procedures laid down in this law. In addition, it shall be admissible to use information regarding facts acquired during criminal proceedings, if such information was obtained and procedurally fixed in

[355] The Biometric Data Processing System Law of the Republic of Latvia, entry into force 24.06.2009, last amendments entry into force 19.07.2017, online version available at https://likumi.lv/ta/en/en/id/193111-biometric-data-processing-system-law, (visited on 31.10.2019).

[356] The Criminal Procedure Law of the Republic of Latvia, entry into force 01.10.2005, last amendments entry into force 25.10.2018, online version available at https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law, (visited on 31.10.2019).

accordance with the procedures laid down in this law (Section 130 (1) of the Criminal Procedure Law). As it is determined in Section 138 (1) of the Criminal Procedure Law investigative actions are procedural actions that are directed toward the acquisition of information or the examination of already acquired information in specific criminal proceedings. An investigative action shall be recorded in minutes, sound, or sound and image recording, but the performer of the investigative action, by recording the course of the investigative action in a sound or sound and image recording, shall notify the persons who participate in the investigative action of such recording before the commencement of the investigative action (Section 141 (1) and Section 143 (1) of the Criminal Procedure Law).

The Biometric Data Processing System is the State Information System the manager and keeper of which is the Information Centre of the Ministry of the Interior. The data (including digital picture of the face[357]) obtained from the following sources shall be included in the Biometric Data Processing System, for example, but not limited to[358]:

- as a result of operative activities, counter-intelligence and intelligence. The obtained data shall be included in the Biometric Data Processing System, if it is necessary in order to prevent risks to the State security and public order, and if a decision regarding enter of such data is taken by the subject of the operative activity who has obtained the relevant data;
- as a result of investigational activities and from detained, suspected, accused and convicted persons;
- from the persons who have no valid personal identification documents after detecting of such factum.

In accordance with Section 10 (1) and (2) of the Biometric Data Processing System Law the following institutions or state authorities of the Republic of Latvia shall ensure inclusion and updating of the data (including digital picture of the face) in the Biometric Data Processing System:

1) the State Police;
2) the Financial Police;
3) the Military Police;
4) the Prisons Administration;
5) the Corruption Prevention and Combating Bureau;
6) customs institutions;
7) the State Border Guard;
8) the State security institutions;

[357] The Biometric Data Processing System Law of the Republic of Latvia, Section 6 and 7.
[358] The Biometric Data Processing System Law of the Republic of Latvia, Section 3 un Section 5 subparagraphs 10), 11), 12).

9) the Road Traffic Safety Directorate;
10) the Maritime Administration of Latvia;
11) the Office of Citizenship and Migration Affairs;
12) the Internal Security Bureau.

Mentioned institutions or authorities shall also be responsible for correct entering of biometric data in the Biometric Data Processing System, and also updating of the included data during the storage thereof. Nevertheless, the Law on the Procedures for Holding the Detained Persons[359] prescribes the procedures for holding the persons detained in accordance with the Criminal Procedure Law (hereinafter - the detained person) at specially equipped police premises - at a temporary place of detention. As stated in Section 3 (8) and 5 (3) 9) of the Law on the Procedures for Holding the Detained Persons prior to placement in the cell, the police official shall take photographs of the detained person and his or her special features and shall prepare a criminalistic characterisation, and the detained person may not refuse from taking photographs.

In accordance with Section 5 subparagraphs 1), 4) and 5) of the Biometric Data Processing System Law the data (including digital picture of the face[360]) obtained from the following sources shall be included in the Biometric Data Processing System, for example, but not limited to:

- when issuing personal identification documents;
- when issuing seafarer identification documents;
- when issuing drivers' licences.

In addition, the purpose of the Personal Identification Documents Law[361] is to determine personal identification documents and documents certifying legal status of persons (hereinafter - the personal identification document) and documents substituting such documents (hereinafter - the temporary document). This law prescribes the types of personal identification documents and temporary documents, procedures for their use, transfer and removal, as well as the rights and obligations of the holder of the personal identification document or temporary document. In accordance with Section 4 (3) of the Personal Identification Documents Law the personal identification document shall include information regarding the person according to the data of the Population Register and biometric data of the person in such amount and format as determined by international legal acts regarding travel

[359] The Law on the Procedures for Holding the Detained Persons of the Republic of Latvia, entry into force 21.10.2005, last amendments entry into force 06.03.2019, online version available at https://likumi.lv/ta/en/en/id/119371-law-on-the-procedures-for-holding-the-detained-persons, (visited on 31.10.2019).
[360] The Biometric Data Processing System Law of the Republic of Latvia, Section 6.
[361] The Personal Identification Documents Law of the Republic of Latvia, entry into force 13.06.2012, last amendments entry into force 09.08.2017, online version available at https://likumi.lv/ta/en/en/id/243484-personal-identification-documents-law, (visited on 31.10.2019), Section 1.

documents. The State information system Information System of Personal Identification Documents shall be used for the issuance, accounting and verification of personal identification documents[362].

In general, facial images collected not as biometric data is governed by the general rules of the Personal Data Processing Law[363] (the GDPR). In practice, each state authority or institution may specify the collection, extent, scope, use and other conditions in their internal regulations.

As it was already specified above, the Processing of Biometric Data Law does not define the subjects from who (which group of natural persons) facial images are collected from, but rather refers to the procedures which are sources of such data, namely[364]:

- when issuing personal identification documents;
- when issuing seafarer identification documents;
- when issuing drivers' licences;
- from non-identified bodies;
- as a result of operative activities, counter-intelligence and intelligence. The obtained data shall be included in the Biometric Data Processing System, if it is necessary in order to prevent risks to the State security and public order, and if a decision regarding enter of such data is taken by the subject of the operative activity who has obtained the relevant data;
- as a result of investigational activities and from detained, suspected, accused and convicted persons;
- from the persons who have no valid personal identification documents after detecting of such factum.

In accordance with Sections 12 and 13 of the Processing of Biometric Data Law the data included in the Biometric Data Processing System shall be restricted access information and shall be used in order to ensure:

1) prevention of the use of another person's identity;
2) verification of the identity of the person in the process of issue of personal identification documents, and also in the process of issue of other documents referred to in this law or figuring out of the person's identity in the process of issue of personal identification documents;
3) determination of the identity of the person during intelligence, counter-intelligence, operative activity, and also during analysis of the obtained information;

[362] The Personal Identification Documents Law of the Republic of Latvia, Section 8 (1).
[363] The Personal Data Processing Law of the Republic of Latvia, entry into force 05.07.2018, last amendments entry into force 31.05.2019, online version available at https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law, (visited on 31.10.2019).
[364] The Biometric Data Processing System Law of the Republic of Latvia, Section 5.

4) prevention of criminal offences and other infringements of the law;
5) detection of criminal offences and search of persons who have committed a criminal offence;
6) verification of the identity of detained, suspected, accused and convicted persons;
7) verification of the identity of the person, when carrying out border check of persons;
8) verification of the identity of the person when carrying out the control of conditions for residing of foreigners;
9) verification of the identity of asylum seekers;
10) biometric identification of non-identified dead bodies (comparison of a sample with all biometric data samples included in the Biometric Data Processing System in order to find out match with one of the biometric data samples included in the Biometric Data Processing System and, if such match is established, in order to find out the identity if the owner of a sample to be compared);
11) searching of missing persons;
12) verification of the identity of the person, when providing a public service to the person, for the provision of which in accordance with the requirements of the laws and regulations it is necessary to carry out verification of the identity of the person. The verification above-mentioned in this subaragraph, when comparing data of the person whom the service is provided, with the data of this person already accumulated in the Biometric Data Processing System, shall be carried out only upon consent by the person;
13) determination of the identity of the person, if it is necessary for the provision of emergency medical care.

The Biometric Data Processing System is the State Information System the manager and keeper of which is the Information Centre of the Ministry of the Interior.[365] But Regulations Regarding Biometric Data Processing System[366] prescribes 1) procedures and amount for including data in the Biometric Data Processing System (hereinafter - the System) by the responsible institutions or state authorities referred to in Section 10 (1) the Biometric Data Processing System Law (please find list above) and updating them, and also conditions for performance of the above-mentioned activities; 2) procedures for destructing biometric data; and 3) procedures and amount for use of the biometric data included in the Biometric Data Processing System by the institution or state authority referred to in Section 14 (1) of the the Processing of Biometric Data Law, namely, the following institutions are entitled to use the Biometric Data Processing System for the performance of the functions abovementioned in Section 13 of this law:

[365] The Biometric Data Processing System Law of the Republic of Latvia, Section 3.
[366] The Cabinet of Ministers of the Republic of Latvia Regulation No. 234 Regulations Regarding Biometric Data Processing System, adopted 06.05.2014, entry into force 09.05.2014, online version available at https://likumi.lv/ta/en/en/id/266013-regulations-regarding-biometric-data-processing-system, (visited on 31.10.2019), Paragraph 1.

1) the State Police;
2) the Financial Police;
3) the Military Police;
4) the Prisons Administration;
5) the Corruption Prevention and Combating Bureau;
6) customs institutions;
7) State Border Guard;
8) State security institutions;
9) the Ministry of Foreign Affairs;
10) the Road Traffic Safety Directorate;
11) the Maritime Administration of Latvia;
12) the Office of Citizenship and Migration Affairs;
13) the Prosecutor's Office;
14) court;
15) the Information Centre of the Ministry of the Interior;
16) in-patient medical treatment institutions included in the Register of Medical Treatment Institutions which ensure provision of emergency medical care;
17) local government police;
18) the Internal Security Bureau;
19) other State and local government institutions, if the use of the Biometric Data Processing System is intended in external law or regulation.

According to Article 34 of the Personal Data Processing Law data may be processed for other purposes than initially collected in the field of criminal law in the following situations:

1) According to rules transposing Directive 2016/680;
2) For use in administrative and civil litigation and in actions of lawfully authorized officials in criminal justice field;
3) To prevent an imminent and substantial threat to public security;
4) In case there is consent of the data subject.

The Processing of Biometric Data Law does not regulate situations when data (including facial images), which has been collected for other (meaning civil) purposes is used in offence proceedings. However, the Criminal Proceedings Law determines the conditions for permissibility of evidence (e.g. it should be lawfully collected), and there is no specific prohibition.

Finally, the Processing of Biometric Data Law determines that provision of data included in the Biometric Data Processing System to foreign competent institutions shall be permissible in compliance with the international agreements binding on the Republic of Latvia and legal act of the European Union. But compliance with the Processing of Biometric Data Law shall be supervised by the Data State Inspectorate in accordance with the procedures laid down in the laws and regulations regarding personal data protection. [367]

3.17. Lithuania

The following laws regarding offence proceedings, regulate the collection and use of facial images (photographs) in Lithuania:

1) The Law on Police of the Republic of Lithuania (*Lietuvos Respublikos policijos įstatymas*)[368].
According to Article 22 of the Law on Police, an official, in the performance of his duties, with the person's consent and / or in the cases provided by law, shall have a right to take photos or videos, as well as, without person's consent and in accordance with the procedure laid down by the Police Commissioner General, to photograph unidentified persons, helpless persons, unidentified corpses, persons at risk, persons in temporary custody, to record their external features, make audio or video recordings and take fingerprints, samples for genetic typing, or samples for comparative testing and identification, and process this personal data.

2) The Law on Criminal Intelligence of the Republic of Lithuania (*Lietuvos Respublikos kriminalinės žvalgybos įstatymas*)[369].
Article 2(8) of the Law on Criminal Intelligence sets a list of ways of collecting criminal intelligence data. Ambush and surveillance are a couple of examples when facial images may be collected by making video recording or taking photographs.

[367] The Biometric Data Processing System Law of the Republic of Latvia, Section 15 and 16.
[368] **Lietuvos Respublikos policijos įstatymas, entry into force 27.10.2000. Online available:** https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111665/asr, accessed 31.10.2019.
[369] Lietuvos Respublikos kriminalinės žvalgybos įstatymas, entry into force 01.01.2013. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.434526/asr, accessed 31.10.2019.

3) The Law on Intelligence of the Republic of Lithuania (*Lietuvos Respublikos žvalgybos įstatymas*)[370]. Under Article 9(2) the intelligence authority is entitled to process various personal data. In addition, Article 13(1) sets that the court may permit the following actions related to personal data (including facial images) collection: monitoring and recording of information, correspondence and other communication between persons transmitted via electronic communications networks; access to, inspection and recording of persons' accommodation, other premises or means of transport; collection of documents or objects or their secret inspection and capture.

4) The Law on Special Investigation Service of the Republic of Lithuania (*Lietuvos Respublikos specialiųjų tyrimų tarnybos įstatymas*)[371].
Article 8(1) empowers the Special Investigation Service to check personal documents (which may include person's image) when necessary for the performance of at least one of the tasks of the Special Investigation Service.

5) The Law on Financial Crime Investigation Service of the Republic of Lithuania (*Lietuvos Respublikos finansinių nusikaltimų tyrimo tarnybos įstatymas*)[372].
Article 7 of the Law on Financial Crime Investigation Service set the functions of Financial Crime Investigation Service which include detection and investigation of actions related to fraudulent or negligent keeping of accounts of taxpayers, actions related to legalization of money or property derived from criminal activity, illegal circulation of securities, other illegal actions related to the financial system, etc. During such investigations of Financial Crime Investigation Service images of data subjects may be collected and used during investigation of suspicious financial activities.

6) The Law on Legal Protection of Personal Data Processed for the Prevention, Investigation, Detection or Prosecution of Criminal Offenses for the Purpose of their Execution or for the Purposes of National Security or Defense of the Republic of Lithuania (*Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas*)[373]. The law

[370] Lietuvos Respublikos žvalgybos įstatymas, entry into force 31.07.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr, accessed 28.10.2019.
[371] Lietuvos Respublikos specialiųjų tyrimų tarnybos įstatymas, entry into force 01.06.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.100816/asr, accessed 28.10.2019.
[372] Lietuvos Respublikos finansinių nusikaltimų tyrimo tarnybos įstatymas, entry into force 01.04.2002. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163326, accessed 28.10.2019.
[373] Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas, entry into

regulates the processing of personal data by the competent authorities of the Republic of Lithuania for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of penalties, as well as protection against and prevention of threats to public security (Article 1(2)). According to Article 8, state authorities may collect biometric data in order to achieve the goals listed above. The law also provides detailed instructions how personal data shall be collected and processed for these specific purposes.

7) The Law on Prosecution Service of the Republic of Lithuania (*Lietuvos Respublikos prokuratūros įstatymas*)[374].

The prosecutor's office may process personal data of data subjects when performing the tasks established in Article 2(2), such as organizing, conducting and directing pre-trail investigation, prosecution on behalf of the State, protection of public interest, etc.

List of laws regarding detention of the persons, which regulate the collection and use of facial images in Lithuania, are the following:

1) The Code of Criminal Procedure of the Republic of Lithuania (*Lietuvos Respublikos baudžiamojo proceso kodeksas*)[375].

As the Code of Criminal Procedure sets rules on the pre-trial and trial stages of criminal proceedings, they also include detention of suspects, the accused (the defendant), therefore, their data, including biometric data, are often collected when investigating the criminal offence, as well as used as evidence (for example, Article 8^1, 20).

2) The Penal Code of the Republic of Lithuania (*Lietuvos Respublikos bausmių vykdymo kodeksas*)[376]. According to Article 43(1), the probation service has the right to process the personal data of convicted persons in the execution of public works sentences. As the exhaustive list of such personal data is not provided, the facial images of convicts may be processed as well.

3) The Law on Legal Protection of Personal Data Processed for the Prevention, Investigation, Detection or Prosecution of Criminal Offenses for the Purpose of Their Execution or for the Purposes of National Security or Defense.

---

force 01.07.2011. Online available: https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr, accessed 29.10.2019.

[374] Lietuvos Respublikos prokuratūros įstatymas, entry into force 01.01.1995. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.5956/asr, accessed 28.10.2019.

[375] Baudžiamojo proceso kodeksas, entry into force 01.05.2003. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr, accessed 29.10.2019.

[376] Bausmių vykdymo kodeksas, entry into force 01.05.2003. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.171368/asr, accessed 29.10.2019.

As mentioned before, under this law, state authorities may collect biometric data of respective data subjects that include persons convicted of a criminal offense (Article 5).

List of laws on issuance and use of identity documents, which regulate the collection and use of facial images in Lithuania, are the following:

1) The Law on Identity Card and Passport of the Republic of Lithuania (*Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas*)[377];

2) The Law on the Legal Status of Foreigners of the Republic of Lithuania (*Lietuvos Respublikos įstatymas dėl užsieniečių teisinės padėties*)[378];

3) The Law on Service Passport of the Republic of Lithuania (*Lietuvos Respublikos tarnybinio paso įstatymas*)[379];

4) The Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Rules on Issuing Driving Licenses for Motor Vehicles (*Lietuvos Respublikos vidaus reikalų ministro įsakymas dėl Motorinių transporto priemonių vairuotojo pažymėjimų išdavimo taisyklių patvirtinimo*)[380];

5) The Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Requirements for Personal Document Photos (*Lietuvos Respublikos vidaus reikalų ministro įsakymas dėl nuotraukų asmens dokumentams reikalavimų patvirtinimo*)[381]

In addition to the above-mentioned legal acts, the Description of the Procedure for the Use of Video Surveillance Cameras and Their Fixed Data in Vilnius City Municipality[382], approved by the Order of the Director of Administration of Vilnius City Municipality, regulating the collection and use of facial images.

According to the laws, the facial images are collected from the following groups of persons:

1) based on the Law on Police of the Republic of Lithuania: any data subject who is involved in police operations (for example, suspects, victims, etc.);

---

[377] Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas, entry into force 02.03.2015. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f26839f08f5011e48028e9b85331c55d/asr, accessed 29.10.2019.

[378] Lietuvos Respublikos įstatymas dėl užsieniečių teisinės padėties, entry into force 30.04.2004. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232378/asr, accessed 29.10.2019.

[379] Lietuvos Respublikos tarnybinio paso įstatymas, entry into force 26.01.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.94414/asr, accessed 29.10.2019.

[380] Dėl Motorinių transporto priemonių vairuotojo pažymėjimų išdavimo taisyklių patvirtinimo, entry into force 17.09.2008. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.327050/asr, accessed 29.10.2019.

[381] Dėl nuotraukų asmens dokumentams reikalavimų patvirtinimo, entry into force 01.01.2003. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.197394/asr, accessed 29.10.2019.

[382] VILNIAUS MIESTO SAVIVALDYBĖS TERITORIJOJE ĮRENGTŲ VAIZDO STEBĖJIMO KAMERŲ IR JŲ FIKSUOTŲ DUOMENŲ NAUDOJIMO TVARKOS APRAŠAS. Online available: https://vilnius.lt/vaktai/GetFile.aspx?DocId=d797487c-e6f6-4229-abf3-1caf01c7938c, accessed 29.10.2019.

2) based on the Law on Criminal Intelligence of the Republic of Lithuania: persons subject to criminal intelligence;

3) based on the Law on Intelligence of the Republic of Lithuania:

- persons whose actions may endanger or threaten the national security, state interests, defense and economic power of the Republic of Lithuania;
- persons who apply for a work permit or access to state or official secret information and who consent to the processing of their personal data;
- persons whose data processing is necessary for the assessment of information on external risk factors, threats or threats to the national security, national interests, defense and economic power of the Republic of Lithuania;
- security authorities of persons whose data are provided by foreign intelligence agencies;
- persons having a service or cooperative relationship with or relating to the intelligence authority;

4) based on the Code of Criminal Procedure of the Republic of Lithuania: victims, suspects, defendants, accused, convicts;

5) based on the Penal Code of the Republic of Lithuania: convicts;

6) based on the Law on Legal Protection of Personal Data Processed for the Prevention, Investigation, Detection or Prosecution of Criminal Offenses for the Purpose of Their Execution or for the Purposes of National Security or Defense: persons known to have committed or intending to commit a criminal offense and persons convicted of a criminal offense;

7) based on the Law of Identity Card and Passport of the Republic of Lithuania: citizens of the Republic of Lithuania who apply for an identity card and / or a passport;

8) based on the Law on the Legal Status of Foreigners of the Republic of Lithuania: a foreigner (a person who is not a citizen of the Republic of Lithuania, regardless of whether or not he / she has the citizenship of any foreign state);

9) based on the Law of Service Passport of the Republic of Lithuania: a person who travels to a foreign country in the performance of his/her duties in the exercise of state or municipal institutions or bodies;

10) based on the Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Rules on Issuing Driving Licenses for Motor Vehicles: an applicant (a person applying for a driving license and having his / her permanent residence in the Republic of Lithuania);

11) based on the Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Requirements for Personal Document Photos: a person applying for a personal document;

12) based on the descriptions of the procedure for the use of video surveillance cameras and their fixed data in various municipalities of the Republic of Lithuania, approved by the orders of the directors of

administration of respective municipalities: a natural person captured by video cameras, who can be identified by the image captured in the video.

The purposes to use facial images depend on legal basis as follows:
1) to carry out tasks and obligations applicable to the police (based on the Law on Police);
2) to solve the challenges of criminal intelligence (based on the Law on Criminal Intelligence);
3) to carry out intelligence, counterintelligence, internal administration by the intelligence authority and to strengthen the national security of the Republic of Lithuania by collecting information on risk factors, threats and submitting it to the institutions ensuring national security and eliminating these risk factors and threats (based on the Law on Intelligence);
4) to perform criminal persecution due to corruption-related crimes, criminal intelligence, corruption prevention, analytical anti-corruption intelligence and other tasks assigned to the Special Investigations Service (based on the Law on Special Investigation Service);
5) to investigate crime, criminal offense (based on the Code of Criminal Procedure);
6) to establish the order of serving the sentence and follow such order (based on the Penal Code);
7) for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the execution of penalties, as well as the protection and prevention of threats to public security (based on the Law on Legal Protection of Personal Data);
8) to issue an identity card and / or a passport (based on the Law on Identity Card and Passport);
9) to establish identity when a foreigner: a) applies for asylum in the Republic of Lithuania; b) is detained for illegal entry into, stay in, residence in, transit to or departure from the Republic of Lithuania; c) is expelled from the Republic of Lithuania or returned to a foreign state;
10) to issue a service passport (based on the Law on Service Passport);
11) to issue a driving license (based on the Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Rules on Issuing Driving Licenses for Motor Vehicles);
12) to issue a personal document (based on the Order of the Minister of the Interior of the Republic of Lithuania on the Approval of Requirements for Personal Document Photos);
13) to ensure public order, public and property security and to implement misconduct prevention (based on the descriptions of the procedure for the use of video surveillance cameras and their fixed data in various municipalities).

According to the above-mentioned laws, the facial images are stored in following databases:
1) The Police Information System (POLIS) and other departmental registers and information systems and, in cases provided by law, in state registers;

2) Criminal Intelligence Information System;

3) databases of detention facilities (prisons, probation offices, etc.);

4) databases of police, court and other authorities;

5) databases of institutions issuing identity documents;

6) databases of Migration Department and State Border Guard Service;

7) databases of the State Enterprise "Regitra", that issues driving licenses;

8) databases of institutions issuing personal documents;

9) databases of the municipalities.

The Law on Legal Protection of Personal Data Processed for the Prevention, Investigation, Detection or Prosecution of Criminal Offenses for the Purpose of Their Execution or for the Purposes of National Security or Defense allows to use data, including facial images, which has been collected for other (civil) purposes to be used in offence proceedings.

In case of exchanging evidences, cross-border cooperation is possible between the countries (government entities) according to the Law on Police and the Law on Legal Protection of Personal Data.

3.18. Luxembourg

The following laws regarding offence proceedings and the detention of persons regulate the collection and use of facial images (a person's photographs) in Luxembourg:

1) Code of Criminal Procedure (*Code de procédure pénale*)[383]. According to Article 33 and Article 39 the **state prosecutor may order** fingerprints and **photographs** of persons who appear to have participated in flagrant crime and from detained persons. Fingerprints and **photographs** collected under these articles **may be further processed by the Police for the purposes of prevention, investigation and detection of criminal offenses**. Article 45 stipulates that taking of fingerprints or photographs must be absolutely necessary to establish the identity of the person arrested. It can only be practiced in the context of an investigation for a flagrant crime or delict or a preliminary investigation or a letter rogatory or the execution of a search order issued by a judicial authority. It must be authorized either by the state prosecutor or by the investigating judge. If the controlled person is not the subject of any judicial

[383] Code de procédure pénale, consolidated version 24.08.2019. Online available: http://data.legilux.public.lu/file/eli-etat-leg-code-procedure_penale-2019-08-24-fr-pdf.pdf, accessed 31.10.2019.

investigation or enforcement measure, the identification report and all documents relating thereto cannot be subject to any conservation measure and are destroyed within six months under the supervision of the state prosecutor. Article 47-2 and Article 51-2 states that the fingerprints and **photographs may be ordered also during the preliminary investigation** by the state prosecutor and **when a preparatory investigation is opened** by the investigating judge. According to Article 48-12 the device used for taking photographs is considered as technical means (a configuration of components which detects signals, transmits them, activates their recording and records the signals) within the meaning of this chapter in the case of an observation made outside a private place.

2) Police Act[384]. According to Article 5 the Police may carry out identity checks on persons targeted by using fingerprints and photographs but this must be absolutely necessary to establish the identity of the person and is subject to prior authorization from the Minister or his delegate. Fingerprints and photographs collected pursuant to this article may be further processed for the purposes of prevention, investigation and prosecution of offenses. If the controlled person is not the subject of any report, any execution or research measure, the identification report and all the documents relating thereto cannot be the subject of any conservation measure and are destroyed within six months under the supervision of the Minister or his delegate.

The law on the identification of natural persons, the national register of natural persons, the identity card, the municipal registers of natural persons (*Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques*)[385] regulates the issuance and use of identity documents (identity card) regarding the collection and use of facial images.

According to the Code of Criminal Procedure regarding offence proceedings, facial images are collected from the following groups of persons: suspects, detained, arrested, accused.

The purposes of using facial images according to the Code of Criminal Procedure and Police Act are: prevention, investigation, detection of criminal offenses and identification.

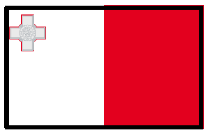
[384] Police Act 2018. Online available: http://legilux.public.lu/eli/etat/leg/loi/2018/07/18/a621/jo, accessed 31/10/2019.
[385] Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques. Online available: http://data.legilux.public.lu/file/eli-etat-leg-memorial-2013-107-fr-pdf.pdf, accessed 31.10.2019.

According to the materials sent by Nathalie Godart, facial images are stored in national database PIC-IMS (Image management system), which is covered by the Code of Criminal Procedure.
Regarding the collection of images by the Police, a video surveillance system called "Visupol" exists in Luxembourg since 2007 and collects images in certain areas of Luxembourg City where the dangerous situations are frequent (traffic, etc..). This system will be amended and the Luxembourg Ministry of Police Affairs recently proposed a new draft law in order to include GDPR requirements and explicitly excluding facial recognition.[386]

The laws of Luxembourg do not allow the use of data, including facial images, which have been collected for other (civil) purposes to be used in offence proceedings[387].

Cross-border cooperation in the case of exchanging evidence is possible between countries (government entities).[388]
Regarding the international cooperation, for the purpose of implementing the Schengen Agreement, the Convention implementing the Schengen Agreement (the "CAS") was signed in the 1990s. This Convention provides for compensatory measures aimed at guaranteeing a single area of security and justice following the abolition of internal border controls. This Convention mainly relates to the provision of legal information with regards to the needs in criminal proceedings one of the measures taken concerns police cooperation. In addition to the CAS, article 45 of the "Traité de Police Benelux" further provides for such cross-border cooperation and spontaneous information exchange between Belgium, the Netherlands and Luxembourg.[389]

3.19. Malta



386 La reconnaissance faciale exclue de la vidéosurveillance, T.Labro. 2019. Online available: https://paperjam.lu/article/reconnaissance-faciale-exclue-.

387 Materials sent by N.Godart, ATTACHÉE - DIRECTION GENERALE - DIRECTION DES RELATIONS INTERNATIONALES -CELLULE JURIDIQUE of Luxembourg Police on 13 August 2019.
388 Ibid.

389 Les pays du Benelux renforcent leur coopération en matière de sécurité avec le nouveau Traité de police Benelux 2018. Online available: https://www.benelux.int/fr/nouvelles/les-pays-du-benelux-renforcent-leur-cooperation-en-matiere-de-securite-avec-le-nouveau-traite-de-police-benelux/.

The judiciary system in Malta is essentially a two-tier system comprising a court of first instance presided over by a judge or magistrate and a court of appeal.[390] It is the duty of the Maltese Police Force (Il-Pulizija ta Malta) to preserve public order and peace, to prevent, detect and investigate offences, to collect evidence and to bring the offenders, whether principals or accomplices, before the judicial authorities.[391]

The following laws regarding offence proceedings, regulate the collection and use of facial images (a person's photographs):

1) Criminal Code[392]. According to Article 355BA the **investigating officer may**, with the appropriate consent in writing of the person arrested, **cause to be taken**: fingerprints, palm-prints, other prints, hand-writing samples or **photographs from the person arrested**. Article 397 stipulates that **the court may**, moreover, at the request of the Police, order that **any accused person be photographed** or measured or that his finger-prints be taken. When an accused person, who has not been previously convicted of crime, is acquitted, all photographs (both negatives and prints), finger-print impressions, and records of measurements so taken, shall be destroyed or handed over to the person acquitted. According to Article 554 **it is lawful for the magistrate to order that any suspect be photographed** or measured or that his fingerprints be taken or that any part of his body or clothing be examined by experts. Article 669 stipulates that notwithstanding any other provision of this Code or of any other law, any process-verbal drawn up in accordance with the provisions of this article including **any photographs**, video recordings and computer images **shall be admissible in evidence in any criminal proceedings** as if it were the property itself described in the procès verbal;

2) Police Act[393]. According to Article 57 **the investigating officer** with the assistance of such competent persons as **may** be necessary and with the appropriate consent, may – **take photographs of the person arrested** or of non-intimate parts of his body. Article 58 states that any person may, within one year from the date of his acquittal by a final judgment of a court, demand that all samples, fingerprints and documents taken from him and any recordings of his voice or photographs or video recordings of him be returned to him or destroyed in his presence. Article 62 stipulates that the **Police may hold, process and classify any information** relevant to the commission of any crime in or outside Malta which information may be preserved by any system whatsoever, including in electronic format, subject to the

[390] Organization of justice – judicial systems, Malta. Available at: https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-mt-en.do?member=1, accessed 20.12.2019.
[391] Europol – Malta, available at: https://www.europol.europa.eu/partners-agreements/member-states/malta, accesed 20.12.2019.
[392] Criminal Code 1854. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574&l=1, accessed 31/10/2019.
[393] Police Act 2017. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8686&l=1, accessed 31/10/2019.

provisions of any law on the protection of data. **Such information may relate to** fingerprints, **photographs**, measurements, blood-samples, intimate or non-intimate samples, patterns of criminal behaviors and methodology in the perpetration of an offence and similar details for the purposes of any future identification of offenders;

3) Data Protection Regulations[394]. These Regulations transpose the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (including facial images) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

The legal act regarding the detention of persons, which regulates the collection and use of facial images/photographs in Malta, is the DETENTION SERVICE REGULATIONS[395]. According to Article 12 for purposes of identification and welfare, a personal record for each detained person shall be prepared and maintained. **Every detained person may be photographed on reception**.

List of legal acts on the issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Malta:
1) PASSPORT REGULATIONS[396]. According to Article 5 Every person applying for a passport shall have his photograph and biometric data taken by an authorized officer;
2) IDENTITY CARD AND OTHER IDENTITY DOCUMENTS ACT[397]. According to this act identity card, residence document and an identification document shall contain a photograph of the person in respect of whom it is issued;
3) MOTOR VEHICLES REGULATIONS[398].

[394] DATA PROTECTION (PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE PURPOSES OF THE PREVENTION, INVESTIGATION, DETECTION OR PROSECUTION OF CRIMINAL OFFENCES OR THE EXECUTION OF CRIMINAL PENALTIES) REGULATIONS 2018. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12840&l=1, accessed 31/10/2019.
[395] DETENTION SERVICE REGULATIONS 2016. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12538&l=1, accessed 31/10/2019.
[396] PASSPORT REGULATIONS 1993. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=9184&l=1, accessed 31/10/2019.
[397] IDENTITY CARD AND OTHER IDENTITY DOCUMENTS ACT 2012. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8751&l=1, accessed 31/10/2019.
[398] MOTOR VEHICLES REGULATIONS 1994. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=9196&l=1, accessed 31/10/2019.

According to legal acts, facial images/photographs are collected from the following groups of persons:

1) Criminal Code – suspects, arrested, accused;

2) Police Act – Arrested;

3) Detention Services Regulations – detained persons.

The main purposes of using facial images, according to the Data Protection Regulations, Criminal Code and Police Act, are: prevention, investigation, detection or prosecution of criminal offences including to preserve public order and peace.

There is no information available to us regarding the exact national database in which the facial images are stored and processed. According to Article 68 of Police Act the custody officer shall keep a register in which shall be recorded such personal details as to enable the identification of any person detained at the police station, but facial images are not mentioned.

The laws in Malta in general allow to use data, including facial images, which has been collected for other purposes to be used in offence proceedings. Regulation 19 of Processing of Personal Data (Electronic Communications Sector) (Amendment) Regulations[399] states that any data retained by service providers shall be disclosed only to the Police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime.[400]

Intelligence services can conduct surveillance as long as it is authorised by a warrant issued by the minister in accordance with Articles 6 of the Security Service Act[401].[402] As long as a warrant is issued in terms of Articles 6 and 7 of the Security Service Act in case of surveillance of individuals and also vis-a-vis private sector, the Security Service can carry out interception of or interference with communications by any means, including post, radio communications or telecommunications."[403]

In reality, facial images can be collected of anyone. For example, at the end of year 2019, several reports read that multiple plain clothes policemen were observed at strategic locations through various ad-hoc

[399] Malta, House of Representatives (2013), Processing of Personal Data (Electronic Communications Sector) (Amendment) Regulations, 2013, 1 January 2013, available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=25839&l=1 (29 August 2014)

[400] Jesuit Centre for Faith and Justice, Charmaine Cristiano Grech, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Malta, available at: https://fra.europa.eu/sites/default/files/fra_uploads/malta-study-data-surveillance-mt.pdf (02.01.2020)

[401] Malta, House of Representatives (1996), Security Service Act, Chapter 391 of the Laws of Malta, 26 July 1996, 6 September 1996, available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8858&l=1 (13 August 2014)

[402] Ibid.

[403] Jesuit Centre for Faith and Justice, Charmaine Cristiano Grech, Op.cit.

protests taking photos and videos of identifiable individuals, while no information was being provided by police about the potential profiling and tagging of individuals or whether any requirement mandated by law are being observed.[404] In addition, in 2016, the Maltese government signed a Memorandum of Understanding with the Chinese telecommunications company Huawei, to install cameras fitted with facial recognition technology.[405] European Commissioner for Justice has written that a planned deployment of a Safe City CCTV network with biometric facial recognition in Malta would have to undergo a data protection impact assessment and comply with GDPR, in order to comply with EU law.[406] "This new form of surveillance technology will utilise Artificial Intelligence (AI) controlled technology to monitor activity and to identify subjects though the use of algorithms that will, supposedly, match the faces of people with established databases. This project will be rolled out and developed by the Maltese State in cooperation with the Chinese tech-giant Huawei."[407]

The UN Special Rapporteur on the right to privacy recommended at the end of 2019 to the Government of Malta to reinforce the protection of fundamental human rights and respect for the rule of law in the context of the reform of its surveillance, policy, legislation and practices.[408] It derives from his statements that Malta's laws need to be reformed so as to introduce greater accountability and better safeguards which would protect privacy, the rule of law and democratic governance in Malta.[409] He made several recommendation, including the creation of an independent Security Commissioner responsible for approving interception warrants and other activities of the Malta Security Service (MSS); the creation of a Security Service Oversight Board consisting of three serving or retired Judges tasked with oversight of the Security Commissioner and the MSS as well as with dealing with complaints from the public about the MSS; and the change of ultimate reporting lines for the MSS from the Prime Minister to the President.[410]

Facial data exchange between EU member states

[404] David Hudson, Police surveillance during protests may be unlawful, IT Law association says (04.12.2019). Available at: https://www.maltatoday.com.mt/news/national/99057/police_surveillance_during_protests_may_be_unlawful_it_law_association_says#.Xg4Nfi2ZNQI (02.01.2020)
[405] Gordon Watson, EC drafting laws to rein in Facial Recognition Technology (23.08.2019). Available at: https://newsbook.com.mt/en/ec-drafting-laws-reigning-in-facial-recognition-technology/ (02.01.2020)
[406] Biometric Update, EU Commissioner warns Malta public facial recognition plan may not meet legal requirements (08.04.2019). Available at: https://www.biometricupdate.com/201904/eu-commissioner-warns-malta-public-facial-recognition-plan-may-not-meet-legal-requirements (02.01.2020)
[407] FRANCOIS ZAMMIT, 'Safe City Malta': Is Privacy the Real Crux of the Matter? (16.01.2019). Available at: https://www.islesoftheleft.org/safe-city-malta-is-privacy-the-real-crux-of-the-matter/ (02.01.2020)
[408] Malta: UN expert recommends broad changes to surveillance laws, GENEVA (18 December 2019). Available at: https://unric.org/it/malta-un-expert-recommends-broad-changes-to-surveillance-laws/
[409] Malta: UN expert recommends broad changes to surveillance laws. Op.cit.
[410] Ibid.

"After Malta joined the Schengen Zone the Police International Relations Unit was recognized as the local contact point for police cooperation matters with other EU States."[411]" Article 649 CC is normally invoked to grant mutual legal assistance (MLA) requests emanating from foreign judicial, investigative, prosecuting or administrative authorities. Malta is party to international treaties on MLA and has signed two bilateral treaties (USA, China). Malta also follows the Harare Scheme Relating to MLA within the Commonwealth."[412] "Malta is able to provide a wide range of assistance, from the serving of summons and documents to the enforcement of confiscation orders, from the hearing of witnesses to search and seizure, from the production of documents to video conference. Assistance is provided unless contrary to domestic law or public policy (Article 649(1) and (5) of the Criminal Code)."[413]" Requests which are executed by the police, namely the collection of evidence and the taking of interviews, are completed within an average timeframe of three weeks. Requests executed by the Attorney General through the issue of investigation, attachment or freezing orders are generally executed within two weeks. Requests involving the hearing of witnesses are fully executed within 3-6 months, depending on the workload of the Courts. The direct transmission of MLA requests between judicial authorities is covered by Article 649 of the Criminal Code."[414] Malta relies on its cooperation through CARIN, INTERPOL, EUROPOL and police- to-police cooperation (see below) to share pre-MLA information.[415] "Joint investigations are possible under Malta's treaties (e.g., EU Convention on MLA and some bilateral treaties)."[416] "Special investigative techniques that are 'non-intrusive' can be conducted upon consent by the Attorney General (Article 435 E (3) of the Criminal Code). Evidence collected under a warrant or investigation order is admissible if the technique was lawfully conduced, though no law addresses the matter."[417]

[411] Europol – Malta, op.cit
[412] Review of implementation of the United Nations Convention against Corruption, Executive summary: Malta. Available at: https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/13-15October2014/V1406823e.pdf (31.10.2019)
[413] Ibid.
[414] Review of implementation of the United Nations Convention against Corruption. Op.cit.
[415] Ibid.
[416] Ibid.
[417] Ibid.

3.20. The Netherlands

The legal system of the Netherlands is based on the French Civil Code with influences from Roman Law and traditional Dutch customary law[418]. There are several binding rules of law that regulate the collection and use of facial images by state (government entity).

The Dutch Implementation Act of GDPR Article 22 (1) determines that pursuant to Article 9 (1) of the GDPR, processing of personal data evidencing racial or ethnic origin, political views, religious or philosophical beliefs, or membership of a trade union, and processing of genetic data, biometric data for the purpose of unique identification of a person, or health data, or data relating to a person's sexual behaviour or sexual orientation is prohibited. However, the prohibition to process special categories of personal data does not apply if the processing is necessary for the institution, exercise or substantiation of a legal claim, or when courts act within the framework of their legal capacity[419]. Furthermore, in view of Article 9, paragraph 2, part g, of the GDPR, the prohibition to process biometric data for the unique identification of a person does not apply if the processing is necessary for authentication or security purposes[420].

Overall, a government entity always must consider the right to portraiture of persons (Article 19, 20 and 21 of the Dutch Copyright Act[421]). In the interests of public safety as well as criminal investigation, images of any kind may be reproduced or made public by or on behalf of the judicial authorities (Article 22 Dutch Copyright Act[422]).

The collected facial images can be used for the determined purposes:

1) In accordance with the Dutch Code of Criminal Procedure and other criminal legislative acts the facial images are collected for the purpose of prevention, detection, prosecution and trial of criminal offences and the establishment of the identity of a body.

[418] Law of the Netherlands. Online available: https://en.wikipedia.org/wiki/Law_of_the_Netherlands, accessed 31/10/2019.
[419] Dutch Implementation Act of GDPR, Article 22. Online available: https://wetten.overheid.nl/BWBR0040940/2018-05-25, accessed 31.10.2019.
[420] Article 29 the Dutch Implemenation Act of GDPR.
[421] Dutch Copyright Act. Online available: https://wetten.overheid.nl/BWBR0001886/2012-01-01, accessed 31.10.2019.
[422] Article 22 of the Dutch Copyright Act.

2) As stated in the Passport Act the facial images are collected for the purpose of identification. According to the Dutch Implementation Act of GDPR the facial images are collected for authentication and security purposes.
3) In Extradition Act the purpose for collection of facial images is identification of claimed persons, however, in Aliens Act 2000 the purpose of collection of facial images is identification of foreign nationals.
4) The laws regarding detention of persons states that the pictures in identity documents can be used for the prevention, detection, prosecution and trial of criminal offences.

The purpose limitation principle (Article 5.1.b GDPR) prevents using personal data for new purposes if they are incompatible with the original purpose for collecting the data. There are now specific laws in the Netherlands that allow the use of data, including facial images, in offence proceedings, which has been collected for other purposes. According to the Dutch law, personal data, including facial images, which has been collected for other (civil) purposes can be used in offence proceedings. For example, identification data gathered during migration procedures can be used in the investigation and prosecution of criminal offences according to the Aliens Act (Vreemdelingenwet 2000)[423].

In 2004 the Dutch Data Protection Authority (CBP) was asked to issue an opinion on the use of face recognition and the use of biometrics for access control to public events, combined with use for police investigations. The CBP did not review in detail the transfer of data to the police and use for justice purposes, and merely assumed that no data other than the data that are currently transferred for investigation purposes are transmitted.[424]

According to the selected below listed Dutch legislative acts, the facial images are collected from the following groups of natural persons:

1) suspects and convicts - according to the binding rules of law set by the Dutch Code of Criminal Procedure laws;
2) detainees - according to the binding rules of law set by the Dutch Code of Criminal Procedure and the Custodial Institutions Act
3) foreign nationals – according to the Alien Act 2000;
4) Dutch citizens – according to the Passport Act and Driver's Licenses Regulation;
5) all natural persons – according to the GDPR and Dutch Implementation Act of GDPR;
6) claimed persons – according to the Extradition Act.

[423] Vreemdelingenwet. Online available: https://wetten.overheid.nl/BWBR0011823/2019-02-27, accessed 31.10.2019.
[424] E. J. Kindt. Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, Springer 2013, p. 561

With regards the collection and use of facial images in offence proceedings there is a special law for the protection of personal data at the police: the Police Data Act (Wpg). The Wpg regulates the processing of personal data for the exercise of police duties by, among others, the National Police, the special investigation services , the Royal Netherlands Marechaussee and the National Criminal Investigation Department. The Dutch Data Protection Authority (CBP) supervises the Wpg.[425]

Facial images can be captured from suspects, convicts, witnesses and aliens on basis of two legal acts, when there is suspicion of criminal activities punishable by a minimum of 4 years in prison:

1) Code of Criminal Procedure (Article 55c)
2) Law for the identity assessment of suspects, convicts and witnesses (Wet identiteitsvaststelling verdachten, veroordeelden en getuigen)[426]

The Dutch Code of Criminal Procedure Article 55c subsection (2) states that the civil servants shall take one or more photographs and fingerprints with a view to establishing the identity of a suspect who has been arrested for a serious offence as defined in Article 67(1) or who is being questioned on account of a serious offence as defined in Article 67(1) without having been arrested. The public prosecutor or the assistant public prosecutor shall order that one or more photographs and fingerprints shall be taken of any suspect, other than the suspect referred to in Article 55c subsection (2), whose identity is in doubt (Dutch Code of Criminal Procedure Article 55c subsection (3)).

In accordance with the Article 55c subsection (4) the photographs and fingerprints, referred to in Article 55c subsections (2) and (3), may also be processed for the prevention, detection, prosecution and trial of criminal offences and the establishment of the identity of a body. Rules pertaining to the processing of photographs and fingerprints, referred to in Article 55c subsections (2) and (3), shall be set by or pursuant to Governmental Decree[427].

Pursuant to the Dutch Code of Criminal Procedure Article 61a subsection (1) measures in the interest of the investigation can be ordered against the suspect detained for investigation, such measures may include taking photos and video recordings. The mentioned measures can only be ordered in the event of a suspicion of a crime as described in Article 67(1)[428].

[425] Law enforcement. Online available: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/politie
[426] Wet identiteitsvaststelling verdachten, veroordeelden en getuigen. Online availble: https://wetten.overheid.nl/BWBR0026180/2010-10-01, accessed 31.10.2019.
[427] Article 55c of the Dutch Code of Criminal Procedure. Online available: https://wetten.overheid.nl/BWBR0001903/2019-08-01, accessed 31/10/2019.
[428] Article 61a of the Dutch Code of Criminal Procedure. Online available: https://wetten.overheid.nl/BWBR0001903/2019-08-01, accessed 31/10/2019.

The rules regarding the implementation of taking the photos and fingerprints of convicted persons and for processing the results thereof are established in the decision establishing the identity of suspects and convicted persons (Besluit identiteitsvaststelling verdachten en veroordeelden)[429]. The decision with regards the identity of suspects and convicted persons Article 2 lists the data necessary for establishing the identity of a suspect or convicted person is processed in the criminal justice database, that includes the photos taken of him/her in accordance with the law[430].

In the detention proceedings the collection and use of facial images takes place in accordance with already mentioned binding rules of law of the Netherlands. In addition, in accordance with the Custodial Institutions Act Article 28 subsection (2) the identity of the detainee shall be determined before and after the visit, unless an official or employee continuously and personally supervises the detainee. The Custodial Institutions Act Article 28 subsection (5) determines that the designated penal institution is authorized to take one or more photos of the detainee. The photos can be used for the production of identification and for the prevention, detection, prosecution and trial of criminal offenses. The detainee is obliged to carry the identification and to show it at the request of an official or employee[431].

In case the detainee is in hospital, the head of the institution is authorized to take one or more photos of the patient. The photos can be used for the production of identification and for the prevention, detection, prosecution and trial of criminal offenses. The nurse is obliged to carry the identification and to show it at the request of a staff member or employee[432]. Same set of rules are applicable to the juvenile with regards the photos. The director of establishment is authorized to take one or more photos of the juvenile. The photos can be used for the production of identification and for the prevention, detection, prosecution and trial of criminal offenses. The young person is obliged to carry the identification and to show it at the request of an official or employee[433].

In relation to the facial image in the passport and identity card, the Passport Act Article 3 subsection (2) states that a travel document is provided with the facial image, two fingerprints and the holder's signature in accordance with rules to be laid down by regulation of a Minister[434].

---

429 Besluit identiteitsvaststelling verdachten en veroordeelden. Online available: https://wetten.overheid.nl/BWBR0026302/2016-06-01, accessed 31/10/2019.

430 Decision with regards the identity of suspects and convicted persons. Online available: https://wetten.overheid.nl/BWBR0026302/2016-06-01, accessed 31/10/2019).

431 Custodial Institutions Act. Online available: https://wetten.overheid.nl/BWBR0009709/2019-01-01, accessed 31.10.2019.

432 Rules regarding detention hospitals. Online available: https://wetten.overheid.nl/BWBR0008765/2019-01-01, accessed 31.10.2019.

433 Rules regarding juvenile detention centres. Online available: https://wetten.overheid.nl/BWBR0011756/2019-01-01, accessed 31.10.2019.

434 Passport Act. Online available: https://wetten.overheid.nl/BWBR0005212/2017-10-01, accessed 31.10.2019.

However, when applying for a driving license, the authority responsible for issuing driving licenses shall consult the personal data of the applicant included in the basic register of persons (Regulation of Driver's Licenses Article 33 (2)[435]). In the driving licence register is included, but not limited to - the passport photo (Regulation of Driver's Licenses Article 145 (1)e). In accordance with the Regulation of Driver's Licences Article 145 (2) the mentioned data is retained after a driver's license has lost its validity[436]. In case the applicant is completing electronic application of the driving licence, the digital passport photo is taken and signature is digitally recorded by a recognized photographer (Regulation of Driver's Licenses Article 173ii(1). In accordance with the Regulation of Driver's Licences Article 173ii (2) the accredited photographer sends the digital passport photo and digitally recorded signature to the Road Traffic Service together with the driver's license number of the applicant's driver's license and possibly his/her e-mail address. Immediately after confirmation of receipt by the Road Traffic Department, the photographer destroys this information[437].

In accordance with the Aliens Act 2000, that regulate admission and expulsion of aliens, the supervision of aliens who are staying in the Netherlands, and border control, Article 106a (1) to the extent that European regulations relating to biometric data do not enable the facial image or fingerprints to be taken and processed, a facial image and ten fingerprints can be taken and processed from a foreign national for the purpose of establishing identity with a view to implementation of this law. The facial image and fingerprints are compared with the facial image and fingerprints in the alien's administration.

The taking and processing of a facial image and fingerprints are exclusively authorized by a Minister, the officials in the border control, the officials in the supervision of foreigners and the Minister of Foreign Affairs Matters insofar as it concerns determining or verifying the identity[438]. But in case the court examines the identity of a person, then such establishing of his/her identity also includes taking one or more photos and fingerprints[439].

According to the Dutch Criminal laws the facial images are stored and processed in the following databases: Criminal law chain database SKDB ("Strafrechtsketendatabank"), facial recognition database CATCH ("Centrale Automatische Technologie voor Herkenning van personen") and FCM

[435] Regulation of Driver's Licenses. Online available: https://wetten.overheid.nl/BWBR0008074/2019-06-14, accessed 31.10.2019.
[436] Article 145 of Regulation of Driver's Licenses .
[437] Regulation of Driver's Licenses, Article 173ii. Online available: https://wetten.overheid.nl/BWBR0008074/2019-06-14, accessed 31.10.2019.
[438] Article 106a of the Aliens Act 2000. Online available: https://wetten.overheid.nl/BWBR0011823/2019-02-27, accessed 31.10.2019).
[439] Article 26 of the Dutch Extradition Act. Online available: https://wetten.overheid.nl/BWBR0002559/2017-03-01, accessed 31.10.2019.

("Fotoconfrontatiemodule"). Furthermore, according to the Passport Act the facial images are stored and processed in decentralized databases per municipality.

Since 2016 , the police have been using the CATCH database to analyse photos of suspects for criminal justice inquiry. This requires the prior permission of the public prosecutor and investigating judge. [440]
The legislative acts of the Netherlands allow the usage of facial images collected in the Netherlands to be used also by other countries (government entities) for the purpose of offence proceedings in these other countries (government entities). Meaning that the cross-border cooperation is possible between the countries (government entities). For instance, the rules regarding international police information exchange can be found in the following international agreements and treaties:

1) Europol Convention;
2) Convention Implementing the Schengen Agreement;
3) Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union;
4) Prüm Decision (Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime).

3.21. Poland

In Poland the legal system is based on the continental legal system. The common courts in Poland are the courts of appeal (*sądy apelacyjne*), provincial courts (*sądy okręgowe*) and district courts (*sady rejonowe*)[441].

The lists of laws regarding offence proceedings, which regulate the collection and use of facial images are (i) the Criminal Code; (ii) the Act on the Police; (iii) the Code of Criminal Procedure; (iv) the Act on Central Anti-Corruption Bureau; (v) the Criminal Executive Code; (vi) the Press Law.

Under Criminal Code several acts against one's privacy are criminalized, for example anyone who pretends to be another person and uses his or her image or other personal data in order to cause property

[440] Police database contains 2.2 million images of 1.3 million people, by Olaf van Miltenburg, published 19.07.2019. Online available: https://tweakers.net/nieuws/155332/politiedatabase-bevat-2-komma-2-miljoen-afbeeldingen-van-1-komma-3-miljoen-mensen.html

[441] https://e-justice.europa.eu/content_member_state_law-6-PL-en.do?clang=en

or personal damage is subject to imprisonment for up to three years.[442] According to point 1 of the article 191a, anyone who records the image of a naked person or a person during sexual activity, using violence, the unlawful threat of violence or deceit for this purpose, or who distributes the image of a naked person or a person during sexual activity without his or her consent, is liable to imprisonment from three months to five years.

In order to perform its statutory tasks, the Police is entitled to process information, including personal data, which includes facial recognition data (photographs, sketches and image descriptions), within the limitations resulting from Article 19.[443] In addition, Central Anti-Corruption Bureau also has a right to process personal data in connection with the prevention and combating of crime, without the knowledge and consent of the data subject.[444] Internal Security Agency whose tasks include recognition, prevention and detection of crimes and the prosecution of their offenders, has the right to legitimize persons in order to establish their identity as well as to observe and record, using technical means, the image of events in public places and the sound accompanying these events during the performance of operational and exploratory activities undertaken under the Act on the Internal Security Agency and the Intelligence Agency.[445]

Photographs of the suspects may be taken to present the pictures of the suspect to other persons for the purposes of his/her identification.[446] . A convicted person may also be subject to measures to identify him or her, in particular: taking photographs.[447]

"Warsaw/Modlin Airport in Poland has launched biometric security gates for automated border checks with facial recognition to prevent fraudulent travel document use and detect known security threats."[448] Polish Police has stated that whether or not they use facial recognition was a secret.[449]

According to point 2 of Article 13 of the Press Law, press cannot publish any personal data and image of individuals against whom preparatory or court proceedings are pending, as well any personal data and

[442] Point 2 of Article 190a of the Criminal Code
[443] Point 1 and 3 of Article 20 of the Act on the Police
[444] Point 1 of Article 22a of the Act on Central Anti-Corruption Bureau
[445] Point 1(1) and 8(2) of Article 5 and point 2 and 6 of Article 23 of the Act on the Internal Security Agency and the Intelligence Agency
[446] Point 2(1) of Article 74 of the Code of Criminal Procedure
[447] Point 1 of Article 79a of the Criminal Executive Code
[448] https://www.biometricupdate.com/201906/airport-biometrics-launched-in-south-korea-and-poland-as-u-s-oversight-board-weighs-benefits; https://blueswandaily.com/warsaw-modlin-airport-installs-new-biometric-border-control-gates/
[449] https://sciencebusiness.net/news/eu-makes-move-ban-use-facial-recognition-systems

image of witnesses, aggrieved and injured parties, unless these persons agree to it. Competent prosecutor or court may allow, due to public interest, to disclose personal data and image of individuals against whom preparatory or court proceedings are pending.[450]

The laws regulating issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images, under Polish legislation are the Act on Identity Cards, the Act on the Passport Documents and Regulation of the Minister of Infrastructure and Construction of 24 February 2016 on issuing documents confirming the right to drive vehicles. Referred laws require a photograph to be provided in order to issue respective identification document. The Act on the Military Service of Professional Soldiers regulates the collection and use of facial images concerning the obligation to provide a photograph for issuance a special ID card that is issued to professional and candidate soldiers.

The following laws regulate the collection and use of facial images by state, which were not listed above: the Labor Code, the Act on Commune Self-government, the Act on Voivodship Self-government, the Act on County Self-government, and the Act on Municipal Guards.

The Polish Parliament (English for *Sejm*), i.e. lower house of parliament, approved a counterterror law on June 10th of 2016. "*The law contains vague provisions extending the right of intelligence agencies to shut down telecommunications networks, block websites deemed to threaten national security, and conduct surveillance of foreign citizens for up to three months—all without prior court approval. The law also widens the definition of terrorist activity and extends the period suspects can be held without charge to 14 days. On January 31, the parliament approved a measure governing surveillance power, allowing for greater access to Polish citizens' electronic data without a court approval.*" [451] Polish legislation expanded access to telecommunication and other digital data and allowed for greater surveillance by police and other agencies and offers scant guidance as to when such powers could be used, reducing restrictions on the use of surveillance by the police.[452] According to the 2016 amendments, the Polish law:

[450] Point 3 of Article 13 of the Press Law

[451] Freedom House, Polish Government Expands Power to Monitor Citizens, Block Internet. Available at: https://freedomhouse.org/article/polish-government-expands-power-monitor-citizens-block-internet?fbclid=IwAR3aRQzr1k8q-TDOsiAlhIkpoWOyP8_UxyHdaRRtnyzTcl_mni0E3b8vE_U (29.12.2019)

[452] Amnesty International, Poland: New surveillance law a major blow to human rights. Available at: https://www.amnesty.nl/actueel/poland-new-surveillance-law-a-major-blow-to-human-rights?fbclid=IwAR0_8Ypw9KgTzlRSXbMa3ATpL41dbkOSKoZF2E-J3W0UTUT6peKCp-yEsp0 (29.12.2019)

- allows the use of intrusive surveillance measures and extends the scope of the so-called "covert investigative methods" on the basis of vague conditions and an unspecified catalogue of crimes;
- allows the use of surveillance tools that capture "online data", that collect and analyze the personal data of internet users, without the obligation to submit an application before each instance of data collection;
- does not contain a requirement of obtaining prior approval from a judge or other independent authority for obtaining telecommunication and online data;
- lacks guarantees for protection of information covered by professional confidentiality obligations such as attorney-client privilege or privilege for journalistic sources;
- makes very difficult, if not impossible, for people to find out whether they are being unlawfully spied on, or to expose abuse of surveillance powers, as the draft does not contain an obligation to notify targeted persons following the conclusion of surveillance.[453]

"For instance, article 10 of the Law on counter-terrorism activities[454] gives officers of the Internal Security Agency, Police and the Border Guard authorisation to collect fingerprints or face image or non-invasive collection of biological material (allowing for the determination of DNA code) of foreigners in case there are doubts regarding their identity or the real purpose of stay in Poland. Collecting such data may also take place when there is suspicion of illegal border crossing by a foreigner or if it is probable that this person intends to stay in Poland illegally. If the non-national is associated by the mentioned institutions with terrorist activities, the biometric data or biological material may be collected by these institutions and then passed to the Border Guard."[455]

More specifically, personal data is collected from professional soldiers[456], every person who is in a public place where monitoring is located[457], employees and persons being in the workplace or in the area around the workplace (which is monitored, an employer is allowed to install video surveillance in case such CCTV is necessary to ensure the safety of the employees, and/or protect property, and/or control

[453] Ibid.
[454] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz. U. z 2018 r. poz. 452 z późn. zm.)
[455] https://www.diva-portal.org/smash/get/diva2:1348294/FULLTEXT01.pdf
[456] Article 48 of the Act on the Military Service of Professional Soldiers; Ustawa o służbie wojskowej żołnierzy zawodowych, entry into force 01.07.2004, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20031791750, accessed 25.10.2019. The data is kept in the form of a briefcase of personal files and a record card. The records may also be kept in electronic form.
[457] Deriving from the Act on Municipal Guards, entry into force 01.01.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971230779, accessed 25.10.2019, the Act on County Self-government, entry into force 01.01.1999, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910578, accessed 25.10.2019 and the Act on Commune Self-government, entry into force 27.05.1990, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900160095, accessed 25.10.2019

the process of production, and/or protect the trade secrets, which disclosure might cause damage to the employer)[458], applicant/submitter regarding documents confirming the right to drive vehicles[459], applicant/submitter of passports[460] and identity cards[461], sentenced persons[462]. According to the Press Law personal data is processed about persons against whom preparatory or judicial proceedings are pending, witnesses and victims.[463] Based on the Code of Criminal Procedure[464] personal data is being processed about accused person, suspect and/or a person requested in an arrest warrant[465].

Chief Commander of the Police, Chief of the Central Investigation Office, Chief of the BSWP, director of the Central Forensic Laboratory of the Police, voivodship commanders (metropolitan) Police, district (municipal and district) police officers, Chief-Rector of the Police Academy in Szczytno and police school administrators are the administrators of personal data in relation to personal data sets created by them for the implementation of statutory tasks.[466] The heads of the Police organizational units referred to in previous sentence, keep a register of systems or data sets in which information is processed, including personal data.[467] The heads of the Police organizational units referred to above, may create or liquidate systems or data sets, other than those specified in the Act on Police, where information, including personal data, is processed in order to implement statutory tasks by the Police.[468]

Central Technical Authority of the National IT System (CTA NITS) is the administrator of the data processed by the NITS, in accordance with art. 10 of the Act of 24 August 2007 on the Participation of the Republic of Poland in the Schengen Information System (Journal of Laws in 2018, item 2162 as amended).[469]

---

458 Deriving from the Labour Code, Kodeks pracy, entry into force 01.01.1975, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19740240141, accessed 25.10.2019

459 Deriving from the regulation of the Minister of Infrastructure and Construction of 24 February 2016 on issuing documents confirming the right to drive vehicles, Rozporządzenie Ministra Infrastruktury i Budownictwa w Sprawie wydawania dokumentów stwierdzających uprawnienia do kierowania pojazdami, entry into force 25.02.2016, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160000231, accessed 25.10.2019

460 Deriving from the Act on Passport Documents, Ustawa o Dokumentach paszportowych, entry into force 28.08.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061431027, accessed 25.10.2019

461 Deriving from the Act on Identity Cards, Ustawa o Dowodach osobistych, entry into force 01.03.2015, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131, accessed 25.10.2019

462 Deriving from the Criminal Executive Code, Kodeks karny wykonawczy, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970900557, accessed 25.10.2019

463 Prawo prasowe, entry into force 01.07.1984. online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19840050024, accessed 25.10.2019

464 Kodeks postępowania karnego, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555, accessed 25.10.2019

465 Kodeks postępowania karnego, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555, accessed 25.10.2019

466 Article 20 of the Act on the Police; Ustawa o Policji, entry into force 10.05.1990, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900300179, accesed 25.10.2019

467 Ibid.

468 Ibid.

469 KOMENDA GŁÓWNA POLICJI, The Right of Data Subjects to Information, available at: http://www.policja.pl/pol/sirene/prawo-osob-do-informac/76188,The-right-of-data-subjects-to-information.html

Video recordings containing personal data are processed only for the purposes of their collection and stored for a period not exceeding 3 months from the date of recording (unless separate provisions provide otherwise), after the 3-month time period the video recordings containing personal data collected as a result of video surveillance should be destroyed - excluding situations in which recordings were secured, in accordance with separate regulations.[470] Registered image of events, not containing evidence allowing the initiation of criminal proceedings or proceedings in cases of misdemeanors or evidence relevant to these proceedings, shall be kept for a period not shorter than 20 days from the date of recording and not longer than 60 days, and then it shall be destroyed.[471] The Labor Code provides that video recordings which are evidence in legal proceedings or the employer knows they may constitute evidence in such proceedings, the 3-month time limit is extended until the final termination of the proceedings, otherwise the video recordings are processed by the employer solely for the purposes of their collection and stored for a period not exceeding 3 months from the date of recording.[472] After the time periods referred to above (3-month time period or the final termination of the proceeding), video recordings containing personal data collected as a result of video surveillance should be destroyed (unless separate provisions provide otherwise).[473]

Under the Code of Criminal Procedure, the usage of facial images is allowed for proceeding purposes (in accordance with art. 74 of the Code of Criminal Procedure, the accused is obliged to undergo external body examinations and other tests not connected with violation of body integrity, it is also allowed, in particular, to take prints from the accused, photograph the accused and show the accused to other people for identification purposes.), in order to narrow down the suspects or determine evidential value of uncovered traces and for the purposes of arresting a warrant.[474]

[470] (1) Article 4b of the Act on County Self-government, Ustawa o samorządzie powiatowym, entry into force 01.01.1999, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910578, accessed 25.10.2019; (2) Article 60a of the Act on Voivodship Self-government, Ustawa o samorządzie województwa, entry into force 01.01.1999, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910576, accessed 25.10.2019; (3) The Act on Commune Self-government, Ustawa o samorządzie gminnym, entry into force 27.05.1990, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900160095, accessed 25.10.2019

[471] Regulation of the Council of Ministers regarding the method of observing and recording events in public places by municipal guards using technical means. Rozporządzenie Rady Ministrów w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską), entry into force 24.12.2009, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20092201720 , accessed 25.10.2019

[472] Article 22^2 of the Labor code, Kodeks pracy, entry into force 01.01.1975, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19740240141, accessed 25.10.2019

[473] Article 22^2 of the Labor code. Op.cit.

[474] Kodeks postępowania karnego, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555, accessed 25.10.2019.

Based on the Criminal Executive Code, the Act on Identity Card, the Polish Passport Act and the Regulation of the Minister of Infrastructure and Construction of 24 February 2016 on issuing documents confirming the right to drive vehicles, the data can be collected for identification purposes. That data includes facial images.

Based on the Act on the Internal Security Agency and the Intelligence Agency and The Act on the Central Anti-Corruption Bureau the data may be collected in order to perform statutory tasks. According to the Act on the Military Service of Professional Soldiers personal data may be processed for identification purposes and/or in order to confirm that a soldier is in full, professional military service. The Act on Municipal Guards stipulates that personal data may be processed in order to perform statutory tasks (referred to in article 11 of the beforementioned Act), in order to record evidence of a crime or an offense, to counter violations of peace and order in public places and/or to protect municipal facilities and utilities.

The Act on the Police brings out that personal data may be processed to perform statutory tasks (referred to in article 1 of the beforementioned Act) and/or in order to exercise the rights related to conduction of administrative proceedings, the implementation of administrative and procedural activities and other activities be carried out by Police officers on the basis of statutes and acts. According to the Act on County Self-government personal data may be processed to ensure public order and security of citizens, as well as to provide fire and flood protection. The Act on Voivodship Self-government[475] allows processing personal data for purposes of protecting property. According to the Act on Commune Self-government personal data may be processed to ensure public order and security of citizens, as well as to provide fire and flood protection.

The Press Law states that the competent prosecutor or court may allow, due to important public interest, disclosure of image and other personal data of persons against whom the preparatory or judicial proceedings are pending. According to the Labor Code, personal data may be processed to ensure safety of employees, to protect property, to control production, and/or to keep confidential information, disclosure of which might expose the employer to detriment.

There are several national databases where facial images are stored and processed, which needs to be taken into account. Data sets, where the Police collects or processes information, including personal

[475] Ustawa o samorządzie województwa, entry into force 01.01.1999, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910576 (25.10.2019)

data, are kept in IT systems or in hard copy, indexes, books, lists, registers, albums or other records.[476] Information collected by the Police in the form of photographs of persons, including images, is processed in sets of album cards or in electronic form in data sets processed in IT systems.[477] The Police Commander-in-Chief keeps a register of data sets and data set sets created in the Police.[478] The Criminal Code[479], The Code of Criminal Procedure, The Criminal Executive Code[480], The Act on the Police, The Act on the Internal Security Agency and the Intelligence Agency are the legal acts which should be taken into account related to whom, when, how and on what basis the information can be revealed and used.

The minister competent for internal affairs maintains the Register of Identity Cards, which is a central register kept in electronic form.[481] In addition, there is a central register of issued and annulled passport documents, which is kept by the minister competent for internal affairs, who is the administrator of the data collected in this register.[482] A central register of drivers is kept by the minister competent for computerization in the ICT system, the minister is the administrator of data and information collected in the records.[483]

It is possible in Poland to use personal data, including facial images, which have been collected for other (meaning civil) purposes to be used in offence proceedings, based on the Act on the Police. Registered image of events, not containing evidence allowing the initiation of criminal proceedings or proceedings in cases of misdemeanors or evidence relevant to these proceedings, shall be kept for a period not shorter than 20 days from the date of recording and not longer than 60 days, and then it shall be destroyed.[484] The head of the Central Anti-Corruption Bureau may create sets of personal data via written request from the Head of the Central Anti-Corruption Bureau or a person authorized by him, and therefore may receive

[476] Article 5 of the Regulation of the Minister of Internal Affairs and Administration on the processing of information by the Police, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji zmieniające rozporządzenie w sprawie przetwarzania informacji przez Policję, entry into force 05.04.2019, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000180 , accessed 25.10.2019

[477] Ibid.

[478] Article 7(1) of the Regulation of the Minister of Internal Affairs and Administration on the processing of information by the Police, op.cit

[479] Kodeks karny, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970880553, accessed 25.10.2019

[480] Ustawa o strażach gminnych, entry into force 01.01.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971230779, accessed 25.10.2019

[481] Article 55 of the Act on Identity Cards, Ustawa o Dowodach osobistych, entry into force 01.03.2015, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131, accessed 25.10.2019

[482] Article 46 of the Act on Passport Documents, Ustawa o Dokumentach paszportowych, entry into force 28.08.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061431027, accessed 25.10.2019

[483] Article 100a of the Traffic Law, Ustawa - Prawo o ruchu drogowym, entry into force 01.01.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970980602, accessed 25.10.2019

[484] Regulation of the Council of Ministers regarding the method of observing and recording events in public places by municipal guards using technical means

data from data sets, including personal data files, kept by public authorities and state or local organizational units free of charge.[485] The controllers of the datasets referred shall provide the Central Anti-Corruption Bureau with data processed therein.[486]

Cross-border cooperation in case of exchanging personal data **is possible** between the countries (government entities) according to the Act on the Police. Point 2aa of Article 20 of the Act on the Police stipulates that in order to carry out its statutory tasks, the Police shall be entitled to exchange information, including personal data, with law enforcement agencies of the Member States of the European Union and other countries, European Union agencies involved in preventing and combating crime, the International Criminal Police Organisation - Interpol and other international organisations on the terms and conditions set out in separate regulations, European Union law and international agreements. The personal information referred in previous sentence includes photographs, sketches and image descriptions.[487] An image of a person may be presented to a testifying person with the purpose of recognition.[488]

Polish law allows personal data Exchange, which includes facial data, between EU member states. The Police, in order to implement statutory tasks, may collect, obtain, store, process, verify, and use information, including personal data, obtained or processed by authorities from other countries and by the International Criminal Police Organization – INTERPOL.[489] According to the Police Act the Police may provide information, including personal data, in order to prevent or combat crime to authorities from other countries or to the International Criminal Police Organization – INTERPOL, in line with the terms and conditions specified in the Act of 16 September 2011 on sharing information with law enforcement authorities from the European Union (Polish Journal of Laws no. 230 item 1371, of 2013 item 1650, and of 2014 item 1199), in the Community Law, and in the provisions of international agreements.[490]

The Minister competent for internal affairs shall determine, by way of ordinance, the methods for processing the personal data (referred on previous paragraph) in databases, specify which police forces are allowed to use the databases, and set out models of the documents to be used in data processing, with due regard given to the need to protect data from unauthorized access, and the conditions to refrain

[485] Article 22a of the **Act on the Central Anti-Corruption Bureau,** Ustawa o Centralnym Biurze Antykorupcyjnym, entry into force 24.07.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040708 , accessed 25.10.2019
[486] Ibid.
[487] Point 2b (3) of Article 20 of the Act on the Police
[488] Point 1 of Article 173 of the Code of Criminal Procedure.
[489] Article 20 (2aa) of the Law of Police
[490] Article 20 (2ab) of the Law of Police

from collecting specific types of information, and in the case of information mentioned in previous paragraph, considering the necessity to comply with the requirements specified by the authorities of other countries or by the International Criminal Police Organization – INTERPOL, in connection with collecting or obtaining such information.[491]

3.22. Portugal

In Portugal traditional legal sources of law hierarchically are the (i) Constitution and constitutional laws; (ii) the rules and principles of general or common international law and international agreements; (iii) laws and decree-laws; (iv) regional legislative decrees; (v) instruments having an effect equivalent to that of laws; and (vi) regulations.[492]

The lists of laws regarding offence proceedings, which regulate the collection and use of facial images are (i) Penal Code (in Portuguese – Código Penal) – DL n.º 48/95, de 15/03 alterado pela Lei n.º 102/2019, de 06/09;[493] (ii) Portuguese Code of Criminal Procedure (Código de Processo Penal) – DL n.º 78/87, de 17/02 alterado pela Lei n.º 102/2019, de 06/09;[494] (iii) Criminal Identification Law (Lei da Identificação Criminal) – Lei n.º 37/2015, de 05/05;[495] (iv) Law no.º 59/2019, de 08/08 – Adopts the rules on the processing of personal data for criminal purposes, transposing the Directive (EU) 2016/680 of 27/04/16;[496] (v) Processing of personal data (Lei n.º 58/2019, de 08/08 – Tratamento de dados pessoais – Execução do Regulamento (EU) 2016/679, de 27/04/16 (DPGR))[497].

The laws governing detention of the persons, which regulate the collection and use of facial images are Internal Rules for Detention Houses (Regulamento Geral dos Estabelecimentos Prisionais – DL n.º

[491] Article 20(19) of the Law of Police (available also from https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e)
[492] https://e-justice.europa.eu/content_member_state_law-6-pt-en.do?member=1, accessed 20.10.2019
[493] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis&so_miolo, accessed 20.10.2019. The laws can be accessed in English via https://gddc.ministeriopublico.pt/pagina/portuguese-legislation-english
[494] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis&so_miolo, accessed 20.10.2019
[495] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2321&tabela=leis&ficha=1&pagina=1&so_miolo, accessed 20.10.2019
[496] https://www.cnpd.pt/bin/legis/nacional/Lei_59_2019.pdf, accessed 20.10.2019
[497] https://www.cnpd.pt/bin/legis/nacional/Lei_58_2019.pdf, accessed 20.10.2019

51/2011, of 11/04, as amended by DL n.º 70/2019, de 24/05[498] and The Law of Lofoscopic and Photographic Judicial Identification (*Identificação Judiciária Lofoscópica e Fotográfica* – Law n.º 67/2017, of 09/08)[499].

The laws regulating issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Portugal are: 1) Portuguese Citizen Card Law (Lei n.º 7/2007, de 05/02 - Cartão de cidadão)[500]; 2) Ordinance no. º286/2017, de 28/09 (Cit. Card) – art. 5.º and Annex III[501]; 3) Legal regime for granting and issuing passports (Decreto-Lei n. º 83/2000, de 11/05 – Regime legal de concessão e emissão dos passaportes)[502]; 4) Driving License Regulation (DL n.º 138/2012, of 05/07, as amended by Retification n.º 3/2018, of 29/01 – *Regulamento da Habilitação Legal para Conduzir*)[503]; 5) National Drivers Registry (DL n. º 262/2009, de 28/09, as amended by DL n. º 12/2017, of 19/01 – *Registo Nacional de Condutores*)[504]; 6) Food and Economic Safety Authority (ASAE) Identification Cards (Portaria n. º161/2019, of 27/05)[505]; 7) Maritime Police Identification Card (Portaria n.º 893/1997, of 11/09 – *Modelo de Bilhete de Identidade da Polícia Marítima*).[506]

Portuguese laws regulating the collection and use of facial images by state (government entity), which are not listed previously are laws regarding facial Images in Military Identification Cards (Navy, Army and Air Force), also in police (P.S.P.), Guarda Nacional Republicana (G.N.R.) and Polícia Judiciária (Judiciary Police) Civil and Military cards as well as cards for Defense Ministry access doors, as stated by the Portuguese national experts. The use of data for purposes other than those which justified their collection requires prior authorization by the CNPD, pursuant to Articles 23(1)(c) and 28(1)(d) of Law 67/98.[507] It should be brought out that facial recognition is used by the Scientific Police Laboratory (Laboratório da Polícia Científica) to control foreign citizens at airports.[508]

[498] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1317&tabela=leis&ficha=1&pagina=1&so_miolo, accessed 22.10.2019
[499] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2736&tabela=leis&so_miolo, accessed 22.10.2019
[500] http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2807&tabela=leis&so_miolo=, accessed 20.12.2019
[501] https://dre.pt/home/-/dre/108228008/details/maximized, accessed 22.10.2019
[502] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1445&tabela=leis&so_miolo, accessed 22.10.2019
[503] http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1757&tabela=leis&so_miolo=, accessed 20.12.2019
[504] www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2633&tabela=leis, accessed 22.10.2019
[505] https://dre.pt/home/-/dre/122403269/details/maximized, accessed 22.10.2019
[506] https://dre.pt/application/file/649990, accessed 22.10.2019
[507] Lei n.º 67/98. Available at: https://dre.pt/web/guest/pesquisa/-/search/239857/details/maximized
[508] Diario de Noticias, Na polícia, no carro, no aeroporto, o reconhecimento facial já não é ficção. Available at: https://www.dn.pt/sociedade/na-policia-no-carro-no-aeroporto-o-reconhecimento-facial-ja-nao-e-ficcao-9047999.html

Travelers are able to cross the border almost seamlessly thanks to face recognition and touchless scanning of fingerprints (called "Biometrics on the Move" technology) which Frontex, the European Border and Coast Guard Agency, started testing it together with Border Service of Portugal (SEF) and the Lisbon Airport Authority (ANA).[509] It is stated by Frontex that this technology will give border guards more time to conduct systematic and efficient security checks without affecting regular travelers, increasing security at the borders.[510]

Based on Law n. º 67/2017, of 09/08, art. º 3º, n. º1, facial images are collected from a) Suspects (arguidos) in criminal procedure: (i) When in doubt about their identity; (ii) If detained preemptively; (iii) Upon judicial dispatch; b) Condemned in criminal process; c) Non-imputable with a security measure; d) Suspects without documents or refuse to identify themselves.

The purposes to use facial images depend from legal basis as follows: prevention, detection, investigation and prosecution of criminal offenses or the execution of criminal sanctions, including protection against threats to public safety and the prevention of such threats (Penal Code, Code of Criminal Procedure and the Law no.º 59/2019).

Recording of identification data such as facial images can be ordered directly by the police. A confirmation of the compulsory measure is not required. In practice, this criminal procedural measure of recording identification data will continue to be the domain of the police and the public prosecutor's office will only deal with resistance on the part of the person concerned.[511] The above mentioned laws allow to use data, which has been collected for other (meaning civil) purposes to be used in offence proceedings.

Databases, in where the facial images are stored and processed are (not conclusive list): Portuguese Electronic Passport Information System (*Sistema de Informação do Passaporte Eletrónico Português*) (SIPOP); Police Information and Operations System (*Sistema de Informações e Operações Policiais*) (SIOP); Platform for Criminal Information Exchange (*Plataforma para o Intercâmbio de Informação Criminal*) (PIIC). Data Centre assists the Schengen Information System, working on the dependency of the Serviço de Estrangeiros e Fronteiras [Boarders and Foreigners Service], under guidance of a

[509] Frontex, Frontex testing the future of border checks at Lisbon airport. Available at: https://frontex.europa.eu/media-centre/news-release/frontex-testing-the-future-of-border-checks-at-lisbon-airport-DI84r4
[510] Frontex, Frontex testing the future of border checks at Lisbon airport. Op.cit.
[511] Information in current paragraph is provided by national expert.

responsible person appointed by the Ministry of Home Affairs.[512] Additionally, it should be brought out that Law nº 10/91 - Law on the Protection of Personal Data in relation to Informatics, is the law that governs what needs to be taken into account in processing personal data, which in principle includes also facial images, via electronic means. "The use of information technology must be carried out in a transparent manner and with strict respect for the reserve of private and family life and for the fundamental rights, freedoms and guarantees of the citizen."[513]

Cross-border cooperation in case of exchanging personal data **is possible** between the countries (government entities) according to the Data Protection Acts.
ACT Nº 36/2003, of 22 August 2003: national legislation implementing the Eurojust Decision, is a national legislation laying down the rules and implementing the Decision of the Council of the European Union 2002/187/JAI of 28 February 2002, setting up Eurojust with a view to reinforcing the fight against serious crime (hereinafter referred to as the Eurojust Decision), regulates the status of the national member of Eurojust, and defines his powers within national territory and his right to act in relation to foreign judicial authorities.

Law enforcement services in Portugal are provided by five different bodies: "Polícia Judiciária" - Criminal Investigations Police - Ministry of Justice: prevention, detection and investigation of violent, organized and financial crime; terrorism; international police cooperation; forensic services; police training; "Guarda Nacional Republicana" - National Gendarmerie; "Policia de Segurança Publica" - Public Security Police; "Serviço de Estrangeiros e Fronteiras" - Immigration and Borders Agency; "Autoridade Tributária" - Customs and Tax Authority.[514] For example one part of the general mission of the Guarda Nacional Republicana is to serve as the national point of contact for international exchange of information on vehicle related crimes with cross-border repercussions. "The Criminal Investigation/Judicial Police (Polícia Judiciária) under the Ministry of Justice has the mission, under the terms of its organic law and the Organisation of Criminal Investigation Act, to assist the judicial and prosecuting authorities in investigations, to develop and foster preventive, detection and investigative actions, falling within their jurisdiction or the actions which the Polícia Judiciária is entrusted with by the competent judicial and prosecuting authorities. The International Co-operation Unit is part of the

[512] Article 5 of the Act 2/94 of 19th of February, which establishes the control and verification mechanisms for the Schengen Information System. Available at: https://www.cnpd.pt/english/bin/legislation/Lei2-94EN.HTM
[513] Article 1 of the Act 10/91 . Available at https://www.cnpd.pt/bin/legis/nacional/lei_1091.htm?fbclid=IwAR34t3V8_IW9ciKs0h-13ByCP8YPhMibAjvFk-98PcxPMn7qmdSkBTOcRIU
[514] Interpol. Available at: https://www.interpol.int/en/Who-we-are/Member-countries/Europe/PORTUGAL

Criminal Investigation Assistance Units." [515] "The Criminal Investigation Police is involved in transnational cooperative criminal investigation activities and illegal migration."[516]

Portuguese Judicial Police working collaboratively and using the secure information exchange systems provided by Europol and INTERPOL, investigators from different agencies including US ICE, Austrian Bundeskriminalamt, French Gendarmerie, Italian Polizia di Communicazioni, UK National Crime Agency and West Midlands Police, Australian Federal Police and Queensland TaskForce Argos, Canada's Toronto Police Service and the Brazilian Federal Police gathered intelligence, led to the arrest of two men who sexually abused children in 2017.[517] That case shows cooperation across borders between polices forces is possible and that personal data (including facial images) can be shared when there is a legal basis (criminal investigation).

3.23. Romania

The following laws regarding offence proceedings, regulate the collection and use of facial images (person's photographs) in Romania:

1) Criminal Procedure Code (*CODUL DE PROCEDURĂ PENALĂ*)[518].

According to the Article 138 of this Code **video, audio or photography surveillance are the special methods of supervision or research**. Video, audio or **photographic surveillance means the photographing of persons**, observation or recording of conversations, movements or other activities. Based on Article 140 of this Code **technical supervision (includes** the video, audio or **photographic surveillance**) may be ordered during the criminal prosecution, for a maximum period of 30 days, at the request of the prosecutor, by the judge of rights and freedoms from the court to which the competence of judging the case in the first instance or from the corresponding court in whose jurisdiction the seat of the prosecutor's office of the prosecutor who made the application is located.

[515] International Centre for Migration Policy Development, Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/doc_centre/police/docs/icmpd_study_lea_infoex.pdf

[516] Helena Machado, Barbara Prainsack; Tracing Technologies: Prisoners' Views in the Era of CSI, page 52.

[517] Europol, Here's How International Collaboration Led to Arrest of Child Sexual Abuser in Portugal. Available at: https://www.europol.europa.eu/newsroom/news/here%E2%80%99s-how-international-collaboration-led-to-arrest-of-child-sexual-abuser-in-portugal

[518] CODUL DE PROCEDURĂ PENALĂ, published 15.07.2010. Online available: http://legislatie.just.ro/Public/DetaliiDocument/120611, accessed 31.10.2019.

2) Law no. 218/2002 for the Organization and Functioning of the Romanian Police (*LEGE nr. 218/2002 privind organizarea □i func□ionarea Poli□iei Române*)[519].

Article 39'2 of that law states that the **Romanian Police is authorized (Note: these provisions will be effective as of 26/01/2020)**:

1) **to fix**, occasionally, **with photo-audio-video** or other technical **means**, operative moments regarding public activities carried out in public places, without the consent of the persons concerned, if there are probable reasons to suspect that in these public places crimes or other illegal acts could be committed or public order and safety disturbed;

2) **to access, directly and free of charge, the systems of surveillance of public spaces** that are installed for crime prevention, security of goods and protection of persons or surveillance of road traffic and which belong to the central or local public administration bodies, except those with responsibilities in the field of national defense and security, when:

a) there are probable causes to suspect that **photographic images** or audio and / or video recordings **processed through these systems can serve to identify**:

- persons who prepare, commit or have committed a crime;
- persons who have been present at the scene of a crime or are aware of the deed, perpetrator or property related to the deed;
- persons pursued or searched according to the law;
- the goods subject to confiscation, forbidden to detention, searched according to the law or which can be used as evidence in a judicial procedure;

b) **photographic images or audio and / or video recordings processed by these systems are necessary for:**

1) establishing and adapting the devices for maintaining the public order, during public meetings or events involving the presence of a large public, as well as for the intervention in case the public meetings lose their peaceful and civilized character;

2) the guidance, supervision and control of compliance with the rules of road traffic;

The processing of personal data contained in photographic images or audio and / or video recordings for purposes other than those in which they were collected is prohibited, except as expressly provided by law and only if the necessary guarantees for the protection of the rights of persons are provided concerned.

The Romanian Police is entitled to keep the photographic images or the audio and / or video recordings obtained according to law for a period of 6 months from the date of obtaining them, except when they are

[519] LEGE nr. 218/2002 privind organizarea □i func□ionarea Poli□iei Române, published 25/04/2014. Online available: http://legislatie.just.ro/Public/DetaliiDocument/35841, accessed 31.10.2019.

used in a judicial procedure, in which case they follow the regime of evidence. When this term is fulfilled, the images and / or recordings are destroyed by irreversible procedures.

3) Law no. 118/2019 regarding the **Automated National Register** for Sexual Offenders (*Lege nr. 118/2019 privind Registrul na□ional automatizat cu privire la persoanele care au comis infrac□iuni sexuale, de exploatare a unor persoane sau asupra minorilor, precum □i pentru completarea Legii nr. 76/2008 privind organizarea □i func□ionarea Sistemului Na□ional de Date Genetice Judiciar*)[520]. According to this Law **the photos of sexual offenders are stored in automated National Register** (Register). The Register represents a means of knowledge, supervision and operative identification of the persons who committed the sexual offenses provided by Criminal Code (Legea nr. 286/2009 Codul Penal[521]).

4) Law no. 363/2018 on the protection of natural persons regarding the processing of personal data by the competent authorities for preventing, discovering, investigating, prosecuting and fighting offenses or executing punishments, educational and security measures, as well as on the free movement of information of these data (*LEGE nr. 363/2018* privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracțiunilor sau al executării pedepselor, măsurilor educative şi de siguranță, precum şi privind libera circulație a acestor date)[522].

Law 363/2018 provides a set of rules on processing personal data to be followed during all phases of criminal trials and applicable to all authorities involved in the prevention, investigation, detection and prosecution of criminal offences, as well as in the execution of criminal penalties. Therefore, the rules apply to police, prosecutors and courts.

Thus, Law 363/2018 provides a series of rules to be followed during the processing of personal data in the field, such as: (i) establishing retention periods; (ii) ensuring the security of personal data; (iii) making a clear distinction between personal data of different categories of data subject such as suspects, convicted persons or victims of criminal offences; (iv) notifying personal data breaches; and (v) appointing a data protection officer.

---

[520] Lege nr. 118/2019 privind Registrul na□ional automatizat cu privire la persoanele care au comis infrac□iuni sexuale, de exploatare a unor persoane sau asupra minorilor, precum □i pentru completarea Legii nr. 76/2008 privind organizarea □i func□ionarea Sistemului Na□ional de Date Genetice Judiciar, published 26.06.2019. Online available: http://legislatie.just.ro/Public/DetaliiDocument/215496, accessed 31/10/2019.

[521] Legea nr. 286/2009 Codul Penal, published 24.07.2009. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/210277, accessed 31.10.2019.

[522] LEGE nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracțiunilor sau al executării pedepselor, măsurilor educative şi de siguranță, precum şi privind libera circulație a acestor date, entry into force 10.01.2019. Online available: http://legislatie.just.ro/Public/DetaliiDocument/209627, accessed 31.10.2019.

5) The law regarding detention of the persons, which regulate the collection and use of facial images in Romania, is: Law no 254/2013 on the execution of punishments and other deprivation of liberty measures ordered by the judicial bodies during the criminal trial (*Lege nr. 254/2013 privind executarea pedepselor □i a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal*)[523].
According to Article 43 of that Law the convicted persons are photographed at the reception in the penitentiary.

List of laws about issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Romania, are the following:

1) Law no. 248/2005 on the free movement of Romanian nationals abroad with subsequent amendments (*Lege nr. 248/2005 privind regimul liberei circula□ii a cetățenilor români în străinătate*)[524];

2) METHODOLOGICAL RULES for the application of Law no. 248/2005 regarding the regime of free movement of Romanian citizens abroad (*NORME METODOLOGICE de aplicare a Legii nr. 248/2005 privind regimul liberei circula□ii a cetă□enilor români în străinătate*)[525];

3) Government Decision no. 556/2006 on the setting up of the date for issuing temporary ordinary passports as well as the form and content of such documents (*HOTĂRÂRE nr. 556/2006 privind stabilirea datei de la care se eliberează pa□apoarte simple temporare, precum □i a formei □i con□inutului acestora*)[526];

[523] Lege nr. 254/2013 privind executarea pedepselor □i a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal, published 14.08.2013. Online available: http://legislatie.just.ro/Public/DetaliiDocument/150699, accessed 31.10.2019.
[524] Lege nr. 248/2005 privind regimul liberei circula□ii a cetățenilor români în străinătate, published 29.07.2005. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/63704, accessed 31.10.2019.
[525] NORME METODOLOGICE de aplicare a Legii nr. 248/2005 privind regimul liberei circula□ii a cetă□enilor români în străinătate, published 27.01.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/205565, accessed 31.10.2019.
[526] HOTĂRÂRE nr. 556/2006 privind stabilirea datei de la care se eliberează pa□apoarte simple temporare, precum □i a formei □i con□inutului acestora, published 02.05.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocument/71142, accessed 31.10.2019.

4) Government Decision no. 557/2006 setting up the date for issuing electronic passports as well as the form and content of such documents (*HOTĂRÂRE nr. 557/2006 privind stabilirea datei de la care se pun în circula□ie pa□apoartele electronice, precum □i a formei □i con□inutului acestora*)[527];

5) Order no. 97/2017 regarding the procedure and the technical conditions in which the records of the examination for obtaining the driving license and the measures for protecting them and the personal data are made and stored (*ORDIN nr. 97/2017 privind procedura □i condi□iile tehnice în care se realizează □i se stochează înregistrările examenului de ob□inere a permisului de conducere □i măsurile pentru protejarea acestora □i a datelor cu caracter personal*)[528];

6) METHODOLOGICAL RULES for the unitary application of the legal provisions regarding the records, domicile, residence and identity documents of Romanian citizens (*NORME METODOLOGICE de aplicare unitară a dispozi□iilor legale privind eviden□a, domiciliul, re□edin□a □i actele de identitate ale cetă□enilor români*)[529];

7) METHODOLOGY of January 26, 2011 on the unitary application of the provisions regarding civil status (*METODOLOGIE din 26 ianuarie 2011 cu privire la aplicarea unitară a dispozi□iilor în materie de stare civilă*)[530].

In addition to the above-mentioned acts the DECISION no. 801 of October 26, 2016 for establishing the procedures for collecting and deleting data of persons with a declared identity, as well as for modifying and completing some normative acts regarding the unitary application of the provisions regarding civil status and the records of persons (*HOTĂRÂRE nr. 801 din 26 octombrie 2016* pentru stabilirea procedurilor de colectare şi ştergere a datelor persoanelor cu identitate declarată, precum şi pentru

[527] HOTĂRÂRE nr. 557/2006 privind stabilirea datei de la care se pun în circula□ie pa□apoartele electronice, precum □i a formei □i con□inutului acestora, published 02.05.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocument/71143, accessed 31.10.2019.

[528] ORDIN nr. 97/2017 privind procedura □i condi□iile tehnice în care se realizează □i se stochează înregistrările examenului de ob□inere a permisului de conducere □i măsurile pentru protejarea acestora □i a datelor cu caracter personal, published 19.08.2017. Online available: http://legislatie.just.ro/Public/DetaliiDocument/192464, accessed 31.10.2019.

[529] NORME METODOLOGICE de aplicare unitară a dispozi□iilor legale privind eviden□a, domiciliul, re□edin□a □i actele de identitate ale cetă□enilor români, published 17.10.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/188152, accessed 31.10.2019.

[530] METODOLOGIE din 26 ianuarie 2011 cu privire la aplicarea unitară a dispozi□iilor în materie de stare civilă, published 02/03/2011. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/220201, accessed 31.10.2019.

modificarea şi completarea unor acte normative privind aplicarea unitară a dispozițiilor în materie de stare civilă şi evidența persoanelor)[531] regulates the collection and use of facial images.

According to Romanian laws the facial images are collected from the following groups of persons:
1) based on Criminal Procedure Code - Suspects, defendants, accused or other persons with whom there is a suspicion that they are related to the crime committed or that they were present at the scene of the crime, even in the absence of their consent;
2) based on Law no. 218/2002 - Persons who prepare, commit or have committed a crime; persons who have been present at the scene of a crime or are aware of the deed, perpetrator or property related to the deed; persons pursued or searched according to the law;
3) based on Law no. 118/2019 – convicted, sexual offenders;
4) based on Law no 254/2013 – convicted persons in the penitentiary;
5) based on all legal acts related to issuance of identity documents - persons applying for an identity document.

The purposes to use facial images depend on legal basis as follows:
1) prevention, detection, investigation, identification or criminal prosecution of the crimes or the execution of the punishments, prevention and combating of other illegal acts, as well as of maintaining the public order and safety (based on Law no. 218/2002, Criminal Procedure Code);
2) preventing and combating sexual acts, exploitation of persons or minors, provided for and punished by the criminal law, as well as to avoid the risk of recidivism (Law no. 118/2019);
3) to prevent the commission of new crimes (based on Law no 254/2013);
4) identification (based on all legal acts related to issuance of identity documents).

According to the above mentioned laws the facial images are stored in following databases:
1) Romanian Police databases (Automated National Register for Sexual Offenders);
2) Electronic storage environment of the electronic passports.

According to Article 97 (1) of the Criminal Procedure Code evidence constitutes any factual element that serves to ascertain the existence or non-existence of a crime, to identify the person who committed it and to know the circumstances necessary for the just settlement of the case and which contributes to finding

[531] HOTĂRÂRE nr. 801 din 26 octombrie 2016 pentru stabilirea procedurilor de colectare şi ştergere a datelor persoanelor cu identitate declarată, precum şi pentru modificarea şi completarea unor acte normative privind aplicarea unitară a dispozițiilor în materie de stare civilă şi evidența persoanelor, published 03.11.2016. Online available: http://legislatie.just.ro/Public/DetaliiDocument/183323, accessed 31.10.2019.

the truth in the criminal case. According to Article 97 (2) the evidence is obtained in the criminal trial by the following means: a) the statements of the suspect or the defendant; b) statements of the injured person; c) statements of the civil party or the civilly responsible party; d) witness statements; e) writings, reports of expertise or finding, minutes, photographs, means of evidence; f) any other means of proof that is not prohibited by law. Law no. 218/2002 **allow to use data, including facial images, which has been collected for other (civil) purposes to be used in offence proceedings.**

Cross-border cooperation in case of exchanging evidences **is possible** between the countries (government entities) **according to the Criminal Procedure Code**, which Article 548 (1) states that international judicial cooperation will be requested or granted in accordance with the provisions of European Union legal acts, international treaties in the field of international judicial cooperation in criminal matters to which Romania is a party, as well as with the provisions contained in the special law and in this chapter, if in the treaties international is not provided otherwise.) and **the Law no. 218/2002** where Article 46 provides that the Romanian police cooperate with similar institutions from other states and with international bodies of profile, based on the agreements to which Romania is a party, including through liaison officers.

3.24. Slovakia

In general, like some newer Member States joined EU in last decade, Slovakia has explicitly provided for some conditions on the processing of biometric data in general data protection legal framework. The data protection legislation of the Slovak Republic expressly states that biometric data may only be processed under the conditions stipulated in a special legislative act and if specified therein for the controller or with the written consent of the data subject.[532] The reference to the need of a legal act in the data protection legislation of the Slovak Republic repeats a requirement which is also stated in Article 8 § 2 ECHR, and that this act will provide for conditions. The provision implies that the legislator supposes that the processing of biometric data interferes with the right to respect for private life.[533]

The following laws regarding offence proceedings, regulate the collection and use of photographs/facial images in Slovakia:

[532] E.J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis. Springer, 2013, p 784-785.
[533] E.J. Kindt. Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis. Springer, 2013, p 784.

1) Data Protection Act (*Zákon o ochrane osobných údajov*)[534];

2) Criminal Procedure Code (*Trestný poriadok*)[535]. Paragraph 126 stipulates that identification of the person or thing can be carried out according to **photographs, possibly using technical means**. According to § 490 (3) the international arrest warrant for the purpose of requesting an accused foreign person for criminal prosecution shall include: the name and surname of the accused, date and place of birth, citizenship, permanent address in the Slovak Republic and other available data facilitating his identification, including his description and **photograph**, or his place of residence abroad.

In addition to the above-mentioned Criminal Procedure Code the following laws are regulating detention of the persons, which regulate the collection and use of facial images in Slovakia:

1) Act on the Execution of Imprisonment (*Zákon o výkone trestu odňatia slobody a o zmene a doplnení niektorých zákonov*)[536]. According to § 40a **the convict's ID card** is intended to identify the convict, regulate the movement and exercise some of the convict's rights, in particular telephoning and purchasing food and personal belongings. **The card contains the photograph**, name, surname, base number and bar code of the convict;

2) Act on Detention (*Zákon o výkone väzby*)[537]. According to the § 30a **the accused's ID card** is intended to identify the accused, regulate movement and exercise some of the accused's rights, in particular telephoning and purchasing groceries and personal belongings. It contains the **photograph**, name, surname, base number and barcode of the accused;

3) Act on Detention Performance (Zakon o výkone detencie)[538] – effective from 01/01/2020. According to § 9 **from detained person may** take fingerprints to verify his or her identity, **take images**, take an external body measurement and identify his or her specific physical features.

List of laws about issuance and use of identity documents, which regulates the collection and use of facial images in Slovakia, is the following:

1) Act on identity cards (*Zákon o občianskych preukazoch*)[539];

---

[534] Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, entry into force 25/05/2018. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/, accessed 31/10/2019.

[535] Trestný poriadok, entry into force 01/01/2006. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/, accessed 31/10/2019.

[536] Zákon o výkone trestu odňatia slobody a o zmene a doplnení niektorých zákonov, entry into force 01/01/2006. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/475/20190701.html, accessed 31/10/2019.

[537] Zákon o výkone väzby, entry into force 01/07/2006. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/221/, accessed 31/10/2019.

[538] Zakon o výkone detencie, entry into force 01/01/2020. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/231/20200101, accessed 31/10/2019.

[539] Zákon o občianskych preukazoch, entry into force 01/07/2006. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/224/, accessed 31/10/2019.

2) Traffic Act (*Zákon o cestnej premávke*)[540].

The groups of people facial images are collected from, are for instance:

1) Persons applying for ID document or driving license (Act on identity cards and Traffic Act);

2) Accused (Criminal Procedure Code and Act on Detention);

3) Convicts (Act on the Execution of Imprisonment);

4) Detained (Act on Detention Performance).

The main purposes to use facial images according to the Criminal Procedure Code are: investigate a crime and identification.

Databases, where the facial images are stored, are kept by the Ministry of Interior of the Slovak Republic. The laws regulating the establishment and usage of these databases are Data Protection Act, Act on identity cards, Traffic Act, Criminal Procedure Code, Act on the Execution of Imprisonment, Act on Detention, Act on Detention Performance.

According the Slovak laws data, including facial images, which has been collected for other (civil) purposes, can be used in offence proceedings, if legally collected. For instance, the Criminal Procedure Code states that state authorities, higher territorial units, municipalities and other legal persons and natural persons are obliged to provide assistance to law enforcement authorities and the court in the performance of their tasks related to criminal proceedings.

Cross-border cooperation in case of exchanging information related to law enforcement matters is possible between the countries (government entities) according to the Criminal Procedure Code. Paragraph 484 stipulates that information may be sent abroad or received from abroad through the Interpol or SIRENE Police Force.

3.25. Slovenia

[540] Zákon o cestnej premávke, entry into force 01/02/2009. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2009/8/

The following laws regarding offence proceedings regulate the collection and use of facial images (a person's photographs):

1) POLICE TASKS AND POWERS ACT (ZAKON O NALOGAH IN POOBLASTILIH POLICIJE)[541]:

- Paragraph 5 of Article 41: Police officers may take the person's photograph, record their personal description and photograph and publish their personal description.
- Paragraph 1 of Article 42: **The identification procedure includes the verification of data kept in the records of the police and administrative bodies** and in other data collections, for the acquisition of which a police officer is authorised by law, as well as **the comparison** of fingerprints and palm prints, **a person's photograph** and personal description, oral mucosa swab and other operative and forensic tasks.
- Paragraph 1 of Article 113: Wherever necessary for the collection of personal or other data to prove minor and criminal offences and identify offenders or perpetrators in accordance with the law, **police** officers **may** in the performance of police tasks **use technical means for taking photographs and making audio and video recordings** and technical means for marking or identifying persons, vehicles and objects used by the police. Recordings that will not be used for proving minor and criminal offences and identifying offences or perpetrators are deleted as soon as possible but no later than within 30 days of their creation.
- Paragraph 1 of Article 114: In order to monitor the legality of the exercise of police powers, **police officers may use technical means for taking photographs** and making video and audio recordings used by the police.
- Paragraph 2 of Article 122 (**Automated processing of personal and other data**) states that any automated processing of personal data, especially the aggregation or comparison of personal data from one or more personal data filings systems (including facial images) in order to make a personality profile of a person is prohibited.

2) Criminal Procedure Act (*Zakon o kazenskem postopku*)[542]:

- Paragraph 2 of Article 149: The police may photograph the person suspected of committing the crime and take their fingerprints. If it is necessary to establish his identity, or in case this is important for the successful completion of the procedure, they may also publish the photograph.

[541] ZAKON O NALOGAH IN POOBLASTILIH POLICIJE, entry into force 05.03.2013. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314, accessed 31.10.2019.

[542] Zakon o kazenskem postopku, entry into force 01.01.1995. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362, accessed 31.10.2019.

- Paragraph 3 of Article 149a: Covert surveillance may be carried out by continuous or repeated observation or tracking using technical positioning and movement devices and **technical devices for transmitting and recording** voice, **photographing and video recording** while focused on monitoring the position, movement and activities of a person. Classified surveillance may be carried out in public and publicly accessible open and closed spaces and places visible from a publicly accessible place or space. Under certain conditions, covert surveillance may also be carried out in private premises if the holder of the premises agrees.

The law regarding the detention of persons, which regulates the collection and use of facial images in Slovenia, is Criminal Enforcement Act (*Zakon o izvrševanju kazenskih sankcij*)[543].

- Paragraph 1 of Article 29: When a convicted person is sentenced, his identity must be identified, criminal record extract obtained, his **photograph taken,** and a medical examination performed.
- Paragraph 1 of Article 29a: When a convicted person is sentenced to house prison, he must be identified, photographed and informed of his rights and duties.

List of laws on the issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Slovenia:
1) Identity Card Act (*Zakon o osebni izkaznici*)[544]
2) Travel Documents Act (*Zakon o potnih listinah*)[545]
3) Drivers Act (***Zakon o voznikih***)[546]

In addition to the abovementioned acts, the Foreigners Act (**Zakon o tujcih**)[547] also regulates the collection and use of facial images.

According to the Criminal Procedure Act, facial images are collected from the following groups of persons: suspects, detainees, accused and convicted.

---

[543] Zakon o izvrševanju kazenskih sankcij. Online available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlid=2006110&stevilka=4665, accessed 31.10.2019.
[544] Zakon o osebni izkaznici, entry into force 28.05.2011. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5758, accessed 31.10.2019.
[545] Zakon o potnih listinah, entry into force. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1598, accessed 31.10.2019.
[546] Zakon o voznikih, entry into force 12.01.2017. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7164, accessed 31.10.2019.
[547] Zakon o tujcih, entry into force 28.07.2011. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5761, accessed 31.10.2019.

The main purpose of using facial images according to the Police Tasks and Powers Act and Criminal Procedure Act is to investigate a crime.

According to the material sent by Gabriel Gajšek from the Slovenian DAPIX delegation on 20 August 2019, facial images are stored in the following databases:
1) Record of photographed persons (persons suspected of having committed a criminal offence);
2) Central record of persons serving prison sentences (convicts).
Slovenian laws allow the use of data, including facial images, which have been collected for other (civil) purposes to be used in offence proceedings, but not with a biometric search.[548]
According to Police Tasks and Powers Act state authorities and legal persons that keep databases pursuant to the law and within or in relation to their activities, must provide the required personal and other data free of charge upon a written or similar demonstrable request from the police, so that the powers and tasks of the police may be exercised and performed and that the interests of the rule of law are protected and effectively implemented.

Cross-border cooperation in the case of exchanging evidence is possible between countries (government entities) according to the Police Tasks and Powers Act.

3.26. Spain

"The sources of the Spanish legal system are the law, custom and general principles of law."[549]
"Custom only applies in the absence of any applicable law, provided that it is not contrary to morality or public order and has been proven."[550]

"Case-law complements the legal system with the doctrine which is repeatedly established by the Supreme Court when interpreting and applying the law, custom and general principles of law."[551]

[548] Material sent by Gabriel Gajšek from Slovenian DAPIX delegation on 20th August 2019.
[549] Spanish legal system and a general overview, online available: https://e-justice.europa.eu/content_member_state_law-6-es-en.do?member=1, accessed 28.10.2019.
[550] Spanish legal system and a general overview, online available: https://e-justice.europa.eu/content_member_state_law-6-es-en.do?member=1, accessed 28.10.2019.
[551] Spanish legal system and a general overview, online available: https://e-justice.europa.eu/content_member_state_law-6-es-en.do?member=1, accessed 28.10.2019.

According to the Spanish Constitution, the primacy of rules under Spanish law is as follows:
- The Constitution
- International Treaties
- Law in the strict sense: Organic Law, ordinary Law and rules with the ranking of Law (including Royal Decree-Law and Royal Legislative Decree)
- Rules emanating from the executive with their own hierarchy depending on the body which issues them (Royal Decree, Decree, Ministerial Order, etc.)[552]

In Spain, the general rules on criminal law are contained in the Penal Code (Organic Law 10/1995, 23 November) and the Law on Criminal Procedure (approved by the Royal Decree of 14 September 1882).

Article 26 of the Organic Law 10/1995 of 23 November 1995 – Criminal Code (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, hereinafter referred to as the Criminal Code),[553] which is an article about evidence, states that for the purposes of the Criminal Code, a document is deemed any material medium that expresses or includes data, facts or narrations that are effective as evidence or of any other kind of legal importance.

For the purposes of Article 132(2)(3) (identification of person against whom the proceedings are filed) of the Criminal Code, the person against whom the proceeding is filed must be sufficiently determined in the court order, either by direct identification or by data that allow subsequent specification of the identification within the organization or group of persons charged with the act.

Following Section 1 of Article 197 of the Penal Code, which states that whoever, in order to discover the secrets or breach the privacy of another, without their consent, seizes their papers, letters, electronic mail messages or any other documents or personal belongings or intercepts their telecommunications or uses technical devices for listening, transmitting, recording or playing sound or image or any other communication signal will be punished with imprisonment of one to four years. Section 2 of the same article stipulates that the same penalties will be imposed upon whoever, without being authorized, seizes, uses or amends, to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in computer, electronic or telematic files or media or in any other kind of file or

[552] Spanish legal system and a general overview, online available: https://e-justice.europa.eu/content_member_state_law-6-es-en.do?member=1, accessed 28.10.2019.
[553] Ley Orgánica del Código Penal, entry into force 24/05/1996, online available: https://www.boe.es/eli/es/lo/1995/11/23/10/con, consolidated text, accessed 28.10.2019.

public or private record. The same penalties will be imposed on whoever, without being authorized, accesses these by any means and whoever alters or uses them to the detriment of the data subject or a third party. Section 3 of Article 197 states that the penalty of imprisonment will be imposed for two to five years if the data or facts discovered or the captured images referred to in Sections 1 and/or 2 are disseminated, disclosed or transferred to third parties. The act will be punished with prison sentences of one to three years, which, with knowledge of its unlawful origin and without having taken part in its discovery, will perform the conduct described in Sections 1 and/or 2 of Article 197. The acts described in Sections 1 and 2 of Article 197 will be punished with a prison sentence of three to five years when:

a) they are committed by the persons in charge or responsible for the files, computer, electronic or telematic media, files or records (originally "personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros"), or
b) they are carried out through the unauthorized use of the victims' personal data.

If the reserved data had been disseminated, transferred or disclosed to third parties, the penalties will be imposed in its upper half. Likewise, according to Section 5 of Article 197, when the facts described in the previous sections (Sections 1-4 of Article 197) affect personal data that reveal the ideology, religion, beliefs, health, racial origin or sexual life, or the victim is a minor or a person with a disability in need of special protection, the penalties provided in its upper half will be imposed. If the facts are carried out for profit, the penalties respectively provided in Sections 1 to 4 of Article 197 will be imposed in the upper half. If they also affect data mentioned in Section 5 of Article 197, the penalty to be imposed will be that of imprisonment for four to seven years. According to Section 7 of Article 197, the act will be punished with a prison sentence of three months to one year which, without authorization of the affected person, disseminates, discloses or transfers to third parties images or audio-visual recordings of the person who would have obtained with their consent at a domicile or any other place outside the reach of the eyes of third parties when the disclosure seriously impairs the personal privacy of that person. Section 8 of Article 197 stipulates that the penalty will be imposed in its upper half when the facts had been committed by the spouse or by a person who is or has been linked to them by an analogous emotional relationship, even without living together, the victim was a minor or a person with a disability in need of special protection or the facts would have been committed for a lucrative purpose.

Article 197 quarter (Article 197c) of the Penal Code rules that if the acts described in this Chapter (TÍTULO X - Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio; CAPÍTULO I - Del descubrimiento y revelación de secretos) have been committed by a criminal organization or group, the higher penalties in degree apply respectively. When, in accordance with the provisions of Article 31

bis, a legal person is liable for the crimes included in Articles 197, 197 bis and 197 ter, the penalty of six months to two years will be imposed. Following the rules established in Article 66 bis, judges and courts may also impose the penalties contained in letters b) to g) of paragraph 7 of Article 33 (Article 197 quinquies (Article 197d)).

Article 198 of the Penal Code states that the authority or public officer who, outside the cases permitted by Law, without there being a legal cause due to an offence having being committed, and availing themselves of their office, acts in any of the manners described in the preceding Article, will be punished with the penalties respectively foreseen therein, in the upper half and with that of absolute barring for a term of six to twelve years. Article 199 of the Penal Code stipulates that whoever discloses the secrets of others that they obtain knowledge thereof through trade or labour relations will be punished with a sentence of imprisonment from one to three years. Professionals who, in breach of their obligation of secrecy or reserve, reveal secrets of another person will be punished with a sentence of imprisonment of one to four years, and special barring from that profession for a term of two to six years.

Article 201 of the Penal Code prescribes that the prosecution of offences foreseen in this Chapter (TÍTULO X - Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio; CAPÍTULO I - Del descubrimiento y revelación de secretos) requires a report by the victim or their legal representative. When the former is a minor, incapacitated or handicapped person, it may also be reported by the Public Prosecutor. The report required in the preceding Section is not necessary to prosecute the acts described in Article 198 of the Penal Code nor when the offence committed affects general interests or persons at large. Forgiveness by the victim or their legal representative, as appropriate, extinguishes the penal action without prejudice to what is set forth in paragraph 2 of subsection 5 of Section 1 of Article 130 of the Penal Code.

Article 35(2) of the Organic Law 5/2000 of 12 January on the criminal responsibility of minors (Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores)[554] (hereinafter referred to as the Organic Law 5/2000) prescribes that the Judge may agree, in the interest of the accused person or the victim, that the sessions are not public and in no case will social media be allowed to obtain or disseminate images of the minor or data that allow their identification. Article 35(3) adds that those who exercise the criminal action in the procedure regulated by this Law must strictly respect the minor's right to confidentiality and non-dissemination of their personal data or the data

[554] Ley Orgánica reguladora de la responsabilidad penal de los menores, entry into force 13.01.2001, online available: https://www.boe.es/eli/es/lo/2000/01/12/5/con , consolidated text, accessed 28.10.2019.

contained in the instruction file under the terms established by the Juvenile Judge. Whoever violates this rule will be the creditor of the civil and criminal responsibilities that may arise. The purpose of Article 35(2) and (3) is to avoid any prejudice for the children, which may result from their defendant status being disclosed to the general public; mass media may neither obtain nor publish images of the child and/or data that allow their identification.[555] "The Judge and the Prosecutor are legally bound to demand strict compliance with Article 35(2) and (3) of the Organic Law 5/2000. Additionally, every participant to the proceedings is obliged to respect the child's right to confidentiality and cannot diffuse their personal data or other relevant information included in the file."[556]

Article 282 bis(7) of the Law on Criminal Procedure – approved by Royal Decree of 14 September 1882 (Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal)[557] (hereinafter referred to as the Law on Criminal Procedure) stipulates that in the course of an investigation carried out by an undercover agent, the competent judge may authorize the obtaining of images and the recording of conversations that may be held in the planned meetings between the agent and the investigated, even if they take place inside a domicile (home). Articles 368-384 bis of the Law on Criminal Procedure are about the identity of the offender and their personal circumstances.

Articles 588 bis a ("Guiding Principles") to 588 bis k ("Destruction of records") of the Law on Criminal Procedure are common provisions for the interception of telephone and telematic communications, the collection and recording of oral communications through the use of electronic devices, the use of technical devices for tracking, locating and capturing images, the registration of mass storage devices and remote records on computer equipment (Chapter IV). Article 588 bis a(1) states that during the investigation of the causes, one of the investigative measures regulated in Chapter IV may be agreed as long as there is judicial authorization issued with full compliance with the principles of specialty, suitability, exceptionality, necessity and proportionality of the measure.

Chapter IV contains Article 588 bis a ("Guiding Principles"), Article 588 bis b ("Request for judicial authorization"), Article 588 bis c ("Judicial resolution"), Article 588 bis d ("Secrecy"), Article 588 bis e ("Duration"), Article 588 bis f ("Request for an extension"), Article 588 bis g ("Measurement control"), Article 588 bis h ("Affectation of third parties") and Article 588 bis i ("Use of the information obtained in

[555] Study on children's involvement in judicial proceedings, online available: http://publications.europa.eu/resource/cellar/841856d7-3c9f-4178-9f42-7dc1c3caadd9.0001.02/DOC_2 , page 18, accessed 28.10.2019.
[556] Ibid.
[557] Real Decreto de por el que se aprueba la Ley de Enjuiciamiento Criminal, entry into force 03.01.1883, online available: https://www.boe.es/eli/es/rd/1882/09/14/(1)/con , consolidated text, accessed 28.10.2019.

a different procedure and casual discoveries") and refers to Article 579 bis, Article 588 bis j ("Cessation of the measure") and 588 bis k ("Destruction of records").

The use of information obtained in a different procedure and casual discoveries is regulated in accordance with the provisions of Article 579 bis of the Law on Criminal Procedure. The Section 1 of Article 579 bis stipulates that the result of the arrest and opening of written and telegraphic correspondence may be used as a means of investigation or evidence in another criminal proceeding. The usage of personal data (facial images) obtained in other procedures in criminal procedures is covered by provision 4 of Law 3/2018, on data protection and digital guarantees. This transitory provision (transposing Directive 2016/680) refers to article 22 of Law 15/1999 on data protection, which covers the regulation of the usage of personal data in criminal procedures. Among other things, this article determines that the data processing without individuals' consent is limited to those circumstances which are necessary for the prevention of a real risk for public security or criminal actions. Whatever falls outside Directive 2016/680 and its transitory provision 4 of Law 3/2018 is regulated by GDPR and its national implementation. **The National Security Act does not state anything specifically about the possibility to use facial recognition when a national security incident occurs, but facial recognition could be used in cases where a national security incident occurs to the extent permitted by the National Security Act.**

Chapter VII (Article 588 quinquies a to Article 588 quinquies c) of the Law on Criminal Procedure is about the use of technical devices for image capturing, tracking and location. Section 1 of the Article 588 quinquies a ("Capturing of images in public spaces or places") brings out that the Judicial Police may obtain and record by any technical means images of the person under investigation when they are in a public place or space, if necessary, to facilitate their identification, locate the instruments or effects of the crime or obtain relevant data for clarification of the facts. Section 2 of Article 588 quinquies a adds that the measure may be carried out even when it affects people other than the investigated person, provided that the utility of surveillance is reduced in a relevant way or there are well-founded indications of the relationship of said persons with the investigated person and the acts which are objects of the investigation. Article 588 quinquies b ("Use of devices or technical means of monitoring and location") stipulates that when accredited reasons of necessity concur, and the measure is provided, the competent judge may authorize the use of technical devices or means of monitoring and locating. The authorization must specify the technical means to be used. It also brings out the exception that there might be an urgent reason to use a device or technical means of monitoring and locating immediately (if the court later decides it was not reasoned, the information obtained from the placed device will have no effect on the process). Article 588 quinquies c ("Duration of the measurement") brings out that the measurement of

the use of technical monitoring and location devices provided for in the previous article have a maximum duration of three months from the date of their authorization. Exceptionally, the judge may agree on successive extensions for the same or a lower term up to a maximum of eighteen months if so justified in view of the results obtained with the measure. The information obtained through the technical monitoring and location devices referred to in the previous articles must be duly guarded to avoid misuse.

Articles 681 and 682 of the Law on Criminal Procedure cover the aspects of the personal data of the victims, witnesses or experts during the oral court proceedings. Article 743 on the other hand covers the recording of the sound and image of the oral court proceeding by the court.

When it comes to detention, it should be brought out that detention and provisional detention must be practiced in the manner that least harms the detainee or prisoner. Those who agree on the measure and those responsible for practicing it as well as subsequent transfers will ensure the constitutional rights to their honor, privacy and image with respect to the fundamental right to freedom of information (Article 520(1) (first paragraph) of the Law on Criminal Procedure – approved by the Royal Decree of 14 September 1882 (Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal[558]).

On legal regulations regarding the issuance and use of identity documents regulating the collection and use of facial images, three laws should be brought out – the Organic Law 7/2015 of 30 March on the Protection of citizen security (Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana)[559] (hereinafter referred to as the Organic Law 7/2015), the Royal Decree 1553/2005 of 23 December ruling the expedition of the national identity document and its electronic signature certificate (Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electronica)[560] (hereinafter referred to as the Royal Decree 1553/2005), and the Traffic Act[561]. According to Articles 8 and 9 of the Organic Law 7/2015, the National Identity Document will include the photograph and signature of its owner and is mandatory from the age of fourteen. According to Article 5(1)(b) of the Royal Decree 1553/2005 to request the issuance of a National Identity Document, the physical presence of the person to whom it is to be issued,

[558] Real Decreto de por el que se aprueba la Ley de Enjuiciamiento Criminal. Op.cit.
[559] Ley Orgánica de protección de la seguridad ciudadana, entry into force 01.07.2015, online available: https://www.boe.es/eli/es/lo/2015/03/30/4/con, consolidated text, accessed 28.10.2019.
[560] REAL DECRETO POR EL QUE SE REGULA LA EXPEDICIÓN DEL DOCUMENTO NACIONAL DE IDENTIDAD Y SUS CERTIFICADOS DE FIRMA ELECTRÓNICA, entry into force 23.12.2005, online available: http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/reales-decretos/real-decreto-1553-2005-de-23-de-diciembre, accessed 28.10.2019.
[561] Real Decreto por el que se aprueba el Reglamento General de Conductores, entry into force 08/12/2009, online available: https://www.boe.es/eli/es/rd/2009/05/08/818/con, consolidated text, accessed 28.10.2019.

the payment of the fee legally established and the presentation of the following documents will be essential along with a color photograph of the applicant's face, size: 32 x 26 millimeters, with a smooth white uniform background, taken from the front with the head completely uncovered without dark glasses or any other garment that may prevent or hamper the identification of the person. Article 7 of the same legal act stipulates that renewing a National Identity Document will be carried out through the physical presence of the owner of the Document, who must pay the corresponding fee and provide a photograph with the characteristics indicated in article 5(1)(b). According to Article 11 of the Royal Decree 1553/2005, the National Identity Document will graphically collect the following data from its owner (on the obverse): surname and name, date of birth, sex, nationality, personal number of the National Identity Document and verification character corresponding to the Tax Identification Number, photograph and signature. Annexes one, two and three of the Traffic Act stipulate the model and content of the European Union driving license, model and content of driving license and what is necessary to obtain and/or extend the permit (different driving authorization) or driving license.

Article 15 of Law 19/2013 of 9 December on transparency, access to public information and good governance (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno)[562] is an article covering data protection. Article 22 of the Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) [563] is about treatments for video surveillance purposes. Article 22(1) stipulates that individuals or legal entities, public or private, may carry out the processing of images through systems of cameras or video cameras in order to preserve the safety of persons and property as well as their facilities. Article 22(3) adds that the data will be deleted within a maximum period of one month from their collection, except when they were to be kept proving the commission of acts that violate the integrity of persons, goods or facilities. In this case, the images must be made available to the competent authority within a maximum period of seventy-two hours after the existence of the recording became known.

Article 22(6) of the same legal act points out that the processing of personal data from images and sounds obtained through the use of cameras and camcorders by the Security Forces and Bodies and the competent bodies for surveillance and control in prisons and for the control, regulation, traffic surveillance and discipline are governed by the legislation transposing Directive (EU) 2016/680, when

[562] Ley de transparencia, acceso a la información pública y buen gobierno, entry into force 10.12.2014, online available: https://www.boe.es/eli/es/l/2013/12/09/19/con, consolidated text, accessed 28.10.2019.
[563] Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, entry into force 07/12/2018, online available: https://www.boe.es/eli/es/lo/2018/12/05/3/con, consolidated text, accessed 28.10.2019.

the treatment is intended for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including protection and prevention against threats to public safety. Outside of these cases, such treatment will be governed by specific legislation and additionally by Regulation (EU) 2016/679 and this organic law.

In the Law on Criminal Procedure approved by the Royal Decree of 14 September 1882 (Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal),[564] there is no certain paragraph pointing out the group of natural persons from whom facial images are collected, but the list would logically cover suspects, accused, victims, police (including but not limited to undercover agents (Article 282 bis 7)), third parties, witnesses and any other person who has legally obtained the image.

There are several purposes for which the use of facial images is allowed:

1) evidence (Criminal Code, Article 26)
2) to prove identity (Royal Decree 1553/2005)
3) oral or sign language interpretation (Law on Criminal Procedure, Article 123 (interpretation))
4) to record the testimonies of witnesses, the purpose of which is not written down but refers logically to the "right to a fair trial" (Law on Criminal Procedure, Article 433)
5) security (Organic Law 4/1997 of 4 August which regulates the use of camcorders by security forces and bodies in public places (Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos)[565]; Law 8/2011 of 28 April which establishes measures for the Protection of Critical Infrastructures (Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas)[566]; and Law 19/2007 of 11 July against violence, racism, xenophobia and intolerance [567])
6) private security (Law 5/2014 of 4 April on Private Security (Ley 5/2014, de 4 de abril, de Seguridad Privada)[568])

[564] Real Decreto de por el que se aprueba la Ley de Enjuiciamiento Criminal. Op.cit.
[565] Ley Orgánica por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, entry into force 06.08.1997, online available: https://www.boe.es/eli/es/lo/1997/08/04/4/con, consolidated text, accessed 28.10.2019.
[566] Ley por la que se establecen medidas para la protección de las infraestructuras críticas, entry into force 30/04/2011, online available: https://www.boe.es/eli/es/l/2011/04/28/8/con, consolidated text, accessed 28.10.2019.
[567] https://www.boe.es/eli/es/l/2007/07/11/19
[568] Ley de Seguridad Privada, entry into force 05.06.2014, online available: https://www.boe.es/eli/es/l/2014/04/04/5/con, consolidated text, accessed 28.10.2019.

7) road safety (Royal Legislative Decree 6/2015 of 30 October which approves the consolidated text of the Law on Traffic, Traffic of Motor Vehicles and Road Safety (Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial)[569])
8) Right to fair trial, legal protection of ones rights (Spanish Constitution (Constitución Española)[570]). The Constitution guarantees the principle of legality, the hierarchy of legal provisions, the publicity of legal enactments, the nonretroactivity of punitive measures that are unfavorable to or restrict individual rights, the certainty that the rule of law will prevail, the accountability of the public authorities, and the prohibition against arbitrary action on the part of the latter. Article 24.2 (Legal protection of your rights) of the Constitution stipulates that all persons have the right of access to the ordinary judge predetermined by law; to the defense and assistance of a lawyer; to be informed of the charges brought against them; to a public trial without undue delay and with full guarantees; to the use of evidence appropriate to their defense; to not make self-incriminating statements; to not declare themselves guilty; and to be presumed innocent.

The Spanish police forces have several databases which may contain facial images for determined situations. For instance: (i) Perpol, a database which contains police records including facial images about individuals;[571] (ii) individuals' identification system (Servicio de identificación), a system which leverages facial images in order to identify individuals;[572](iii) missing persons and unidentified human system, a system used to identify missing persons primarily.[573]

The purpose of Law 37/2007 of 16 November on the reuse of public sector information (Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público)[574] is the basic regulation of the legal regime applicable to the reuse of documents prepared or guarded by public sector

[569] Real Decreto Legislativo por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, entry into force 31.01.2016, online available: https://www.boe.es/eli/es/rdlg/2015/10/30/6/con, consolidated text, accessed 28.10.2019.

[570] Constitución Española, entry into force 29.12.1978, online available: https://www.boe.es/eli/es/c/1978/12/27/(1)/con , consolidated text, accessed 28.10.2019.

[571] Cuerpo Nacional De Policía, Derecho de acceso al fichero "PERSONAS". Available at: https://sede.policia.gob.es/portalCiudadano/cancelacion_antecedentes/derecho_acceso_perpol.html

[572] Cuerpo Nacional De Policía, Servicio de Identificación. Available at: https://www.policia.es/org_central/cientifica/servicios/id_identificacion.html

[573] INFORME "Personas desaparecidas", España (2018). Available at: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/060318INFORME_PERSONASDESAPARECIDAS.pdf ; National Missing Persons Centre, About Us. Available at: https://cndes-web.ses.mir.es/publico/Desaparecidos/en/Nosotros

[574] Ley sobre reutilización de la información del sector público, entry into force 17.01.2008, online available: https://www.boe.es/eli/es/l/2007/11/16/37/con, consolidated text, accessed 28.10.2019.

administrations and organizations. Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas)[575] stipulates that administrations must collect documents electronically through their corporate networks or through consultation with data intermediation platforms or other electronic systems enabled for this purpose. Governmental databases are also governed by the Resolution of 22 December 2003 of the Secretary of State of the Treasury, which issued instructions for the establishment of stable channels of collaboration between the General Directorate of Cadastre and the State Agency for Tax Administration in the field of information exchange and direct access to the respective databases (Resolución de 22 de diciembre de 2003, de la Secretaría de Estado de Hacienda, por la que se dictan instrucciones para el establecimiento de cauces estables de colaboración entre la Dirección General del Catastro y la Agencia Estatal de Administración Tributaria en materia de intercambio de información y acceso directo a las respectivas bases de datos)[576].

There are no laws in Spain excluding the right to use data, including facial images, which have been collected for other (civil) purposes to be used in offence proceedings nor the right to use facial images collected in Spain to be used by other countries (government entities) for the purpose of offence proceedings in these countries.

3.27. Sweden

The following laws regarding offence proceedings, regulate the collection and use of facial images in Sweden:

1) The Swedish Code of Judicial Procedure (Rättegångsbalk (1942:740))[577]. According to Chapter 28 Section 14 **A person arrested or detained may be photographed**, and fingerprinted;

[575] Ley del Procedimiento Administrativo Común de las Administraciones Públicas, entry into force 02.10.2016, online available: https://www.boe.es/eli/es/l/2015/10/01/39/con, consolidated text, accessed 28.10.2019.

[576] Resolución de la Secretaría de Estado de Hacienda, por la que se dictan instrucciones para el establecimiento de cauces estables de colaboración entre la Dirección General del Catastro y la Agencia Estatal de Administración Tributaria en materia de intercambio de información y acceso directo a las respectivas bases de datos, entry into force 22/12/2003, online available: https://www.boe.es/eli/es/res/2003/12/22/(3), accessed 28.10.2019.

[577] Rättegångsbalk (1942:740), entry into force 01/01/1948. Online available: https://www.government.se/49e41c/contentassets/a1be9e99a5c64d1bb93a96ce5d517e9c/the-swedish-code-of-judicial-procedure-ds-1998_65.pdf, accessed 30.10.2019.

2) Police data law (Polisdatalag (2010:361))[578]. According to Chapter 4 Section 13 **Fingerprint and signaling registers may contain information about**: fingerprint, signal element, **photograph**, **video recording**, identification information, case number and crime code;

3) Regulation on fingerprints and alike (Förordning (1992:824) om fingeravtryck m.m.)[579]. According to Section 2 Fingerprints and photography shall, with the support of the provisions of Chapter 28 Section 14 of the Code of Judicial Procedure, is taken by the person who has been:

- arrested as a suspect for a crime,
- arrested as a suspect for a crime, if the arrested person is unknown and refuses to state his name, domicile or time of birth or provides information on these circumstances which may be assumed to be false,
- arrested as suspected of crime, if fingerprints or photograph may be needed to investigate whether the arrested person has committed the crime or any other crime or otherwise to obtain the required investigation or if the arrested person is considered dangerous to public safety or law enforcement.

If it is necessary to investigate crimes in which prison can follow, fingerprints and photographs may also be taken by the person suspected of the crime without being arrested or detained for this and by the person not suspected of the crime;

4) Crime data law (Brottsdatalag (2018:1177))[580]. According to Chapter 1 Section 3 The Act **applies to such processing of personal data that is fully or partially automated** and to other processing of personal data contained in or intended to be included in a structured collection of personal data that **is available for searching or compiling according to specific criteria.** Chapter 2 Section 12 stipulates that Biometric data (personal data relating to a person physical, physiological or behavioral characteristic, such as developed by special technical treatment and enabling or confirms unique identification of person) and genetic data may be processed only if specifically prescribed and it is absolutely necessary for the purpose of the treatment;

5) Complementary law to the GDPR (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning)[581] (Chapter 3: Processing of certain categories of personal data);

---

[578] Polisdatalag (2010:361), entry into force 01.03.2012. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/polisdatalag-2010361_sfs-2010-361, accessed 30.10.2019.

[579] Förordning (1992:824) om fingeravtryck m.m., entry into force 01.08.1992. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-1992824-om-fingeravtryck-mm_sfs-1992-824, accessed 30.10.2019.

[580] Brottsdatalag (2018:1177), entry into force 01.08.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177, accessed 30.10.2019.

[581] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, entry into force 25.05.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218, accessed 30.10.2019.

6) Complementary regulation to the GDPR (Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning)[582]. According to Section 5 Personal data referred to in Article 10 of the EU Data Protection Regulation may be processed by persons other than authorities if the processing is necessary for:

- legal claims can be established, enforced or defended, or
- legal obligation under law or regulation performed.

Section 6 stipulates that Data Inspectorate may issue additional regulations in which cases other than authorities may process personal data referred to in Article 10 of the EU Data Protection Regulation and also decide in individual cases that other persons than authorities may process such personal data.

In addition to the Swedish Code of Judicial Procedure, Crime data law and Regulation on fingerprints mentioned above, there is one more law regarding detention of the persons, which regulates the collection and use of facial images: 'Law with special regulations regarding young criminals' (Lag (1964:167) med särskilda bestämmelser om unga lagöverträdare)[583]. According to Section 36 If a person is suspected of having committed a crime before the age of fifteen, if there are special reasons, seizures, house search and body visitation against the young person, **photography** and fingerprints shall be taken by him or her in accordance with the provisions of Code of Judicial Procedure.

List of laws about issuance and use of identity documents (passport, identity card, driving license), which regulate the collection and use of facial images in Sweden, is the following:

1) Passport Law (Passlag (1978:302))[584];

2) Passport Regulation (Passförordning (1979:664))[585];

3) Driving License Law (Körkortslag (1998:488))[586];

4) Aliens Data Law (Utlänningsdatalag (2016:27))[587].

[582] Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning, entry into force 25.05.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219, accessed 30.10.2019.

[583] Lag (1964:167) med särskilda bestämmelser om unga lagöverträdare, issued 20.03.1964. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-1964167-med-sarskilda-bestammelser-om-unga_sfs-1964-167, accessed 30.10.2019.

[584] Passlag 1978:302, issued 25.05.1978. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/passlag-1978302_sfs-1978-302, accessed 30.10.2019.

[585] Passförordning (1979:664), issued 28.06.1979. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/passforordning-1979664_sfs-1979-664, accessed 30.10.2019.

[586] Körkortslag (1998:488), entry into force 01.10.1998. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/korkortslag-1998488_sfs-1998-488, accessed 30.10.2019.

[587] Utlänningsdatalag (2016:27), entry into force 12.02.2016. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/utlanningsdatalag-201627_sfs-2016-27, accessed 30.11.2019.

The Law on camera surveillance (Kamerabevakningslag (2018:1200))[588] is also regulating the collection and use of facial images.

According to laws regarding offence proceedings the facial images are collected from the following groups of persons:

1) Based on The Swedish Code of Judicial Procedure (Chapter 28 Section 14):

- arrested on suspicion of crime;
- detained on suspicion of crime; or
- others, if necessary to obtain information about an offence punishable by imprisonment.

2) Based on Regulation on fingerprints (Section 2):

- arrested on suspicion of crime;
- detained on suspicion of crime and refuses to state personal details or the photography is needed to investigate the crime;
- suspect without being arrested, if prison may follow and it's needed to investigate the crime.

The purpose to use facial images according to the Swedish Code of Judicial Procedure is to investigate a crime.

Sweden has transposed Directive (EU) 2016/680 with national law (2018:1177)[589] and Law on the police's treatment of personal data within the field of the crime (2018:1693)[590] and has regulated amongst other things the Swedish Police Authority's processing of biometric data e.g. by use of facial recognition technology.[591]

SFS 2018:1177 applies to such processing of personal data (also biometric data) that is fully or partially automated and to other processing of personal data contained in or intended to be included in a structured collection of personal data that is available for searching or compiling according to specific criteria (Chapter 1 Section 3). According to Chapter 1 Section 6 the meaning of processing (also automated) of personal data is: collection, registration, organization, structuring, storage, processing or

588 Kamerabevakningslag (2018:1200), entry into force 01.08.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200, accessed 30.10.2019.
589 Crime data law (2018:1177).
590 Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, entry into force 01.01.2019. Online available: http://rkrattsbaser.gov.se/sfst?bet=2018:1693, accessed 30.10.2019.
591 Based on materials sent by Swedish Police on 24.09.2019.

change, development, reading, use, disclosure, dissemination or other services way, adjustment, merge, restriction, deletion or destruction.
Chapter 2 Section 12 allows to process biometric data and genetic data only if it is specifically prescribed and it is absolutely necessary for the purpose of the treatment.

According to SFS 2018:1693 Chapter 5 Section 14 Fingerprint and signaling registers may contain information about 1. fingerprint, 2. signalment, 3. **photograph**, 4. video recording, 5. identification information, 6. case number, and 7. crime code. Chapter 5 Section 23 stipulates that the police authority may keep a register of information on persons who have been granted an entrance ban in sporting events (the entry ban register) for the purpose of preventing, preventing or detecting violations. The entry ban register may contain the following information about a person who has been granted an entry ban: 1. name, 2. social security number or coordination number, 3. census address and other permanent address, 4. alias, 5. **photograph**, 6. connection to sports and sports organization, 7. the scope and validity of decisions on access bans, 8. violation of the current bans.

According to the Swedish laws the facial images are stored in the following databases:
1) The police's fingerprint and description register (based on Law on the police's treatment of personal data within the field of the crime);
2) Prohibited access register (based on Police data law);
3) Register of national identity cards (based on Förordning 2005:661 om nationellt identitetskort[592]);
4) Migration Board's register of fingerprints and photographs (based on Aliens Data Law).

For more information regarding to different registers in Sweden can be found on the webpage of Swedish Police (https://polisen.se/lagar-och-regler/behandling-av-personuppgifter/polisens-register/).

In addition to the laws mentioned above the following laws allow to use personal data, including facial images, which has been collected for other (civil) purposes to be used in offence proceedings:
1) Law on electronic communication (Lag (2003:389) om elektronisk kommunikation)[593];

[592] Förordning (2005:661) om nationellt identitetskort, entry into force 01.10.2005. Online available: http://rkrattsbaser.gov.se/sfst?bet=2005:661, accessed 30.10.2019.
[593] Lag (2003:389) om elektronisk kommunikation, entry into force 25.07.2003. Online available: http://rkrattsbaser.gov.se/sfst?bet=2003:389, accessed 30.10.2019.

2) Law on gathering of electronic communication data by the law enforcement agencies' intelligence services (Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet)[594].

Cross-border cooperation in case of exchanging evidences is possible between the countries (government entities) according to the Crime Data Law and the Law on the police's treatment of personal data within the field of the crime.

3.28. The United Kingdom

The United Kingdom (the UK) consists of three jurisdictions with separate legal systems: England and Wales, Scotland and Northern Ireland. In England, Wales and Northern Ireland there is a common law legal system, that is based on statute and precedents through case law by judges, however, in Scotland there is a mixed civil and common law system[595]. In certain areas, Welsh Law is devolved and can be distinct from English Law.

Collection and use of facial images regarding detention and offence proceedings

England and Wales

The use of facial recognition technology is governed by a legal framework comprising a combination of statute, common law, legislation, code and guidance and police inner regulations. As a result, there is no individual regulation or governing body that single-handedly regulates the use of facial recognition technologies, instead such activities fall within the scope of various regulations and governing bodies set out herein.

[594] Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, entry into force 01.07.2012. Online available: http://rkrattsbaser.gov.se/sfst?bet=2012:278, accessed 30.10.2019.

[595] Legal systems in the UK: overview, by Professor Suzanne Rab, Serle Court, Dec 2019. Online available: https://uk.practicallaw.thomsonreuters.com/5-636-2498?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, accessed 15.12.2019.

The use of live facial recognition (LFR) technology involves the processing of personal data and therefore data protection law applies (Data Protection Act 2018 (**DPA**)), whether it is for a trial or routine operational deployment. The processing of personal data by 'competent authorities' (s30 DPA 2018) for 'the law enforcement purposes' (s31 DPA 2018) is covered by Part 3 of the DPA 2018[596].
The use of LFR is also regulated by Human Rights Act 1998[597] (HRA) and Equality Act 2010[598]. Article 8 of HRA stipulates that everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

As a public authority, the Metropolitan Police Service (MPS) must comply with Section 149 of the Equality Act 2010 which is most commonly known as the Public Sector Equality Duty. Particular attention is needed in two respects: the technical performance and the operational deployment of the LFR system[599].

When considering the use of LFR, Authorizing Officers will need to assess and minimize any impact on the wider public as follows[600]:

a) LFR cannot be used to identify persons unless they have been included on a Watchlist;

b) The creation of any Watchlist is specific to each Deployment of LFR. This is to ensure the currency, relevancy, necessity and proportionality by which any image is included for potential matching. Images on a Watchlist will be lawfully held by the MPS with all reasonable steps being taken to ensure that the image is of a person intended for inclusion on a given Watchlist;

c) On adding an image to the Watchlist the LFR system will assess the image for quality and suitability for matching in order to allow MPS personnel to consider and manage the risk of poor quality images generating inaccurate LFR Alerts;

---

596 Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places, 31.10.2019. Online available: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.
597 Human Rights Act 1998. Online available: http://www.legislation.gov.uk/ukpga/1998/42/contents, accessed 31.10.2019.
598 Equality Act 2010. Online available: http://www.legislation.gov.uk/ukpga/2010/15/contents, accessed 31.10.2019.
599 LIVE FACIAL RECOGNITION: LEGAL MANDATE, version 1-01. Online available: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mps-lfr-legal-mandate-v1-1.pdf.
600 LIVE FACIAL RECOGNITION: LEGAL MANDATE. Op.cit.

d) The cameras used in the LFR system are of sufficient quality for the LFR system's needs;

e) The LFR system is 'closed' and not connected to other MPS systems or the internet;

f) The LFR system is designed to assist MPS personnel to make identifications. The LFR system will always flag potential matches to at least one member of MPS personnel for a decision on any further action rather than autonomously taking a decision on any action after making a potential match;

g) LFR Deployments and the materials that support LFR Deployments will be subject to periodic review to ensure that the LFR system and its operation remains necessary, proportionate and effective in terms of meeting its use case[601].

The police is one of those competent authorities that is collecting and using facial images in investigation, detection and prevention of crime and terrorist activities as well as safeguarding under the Police and Criminal Evidence Act 1984 ("PACE"). In accordance with PACE section 64A (1) and (1A) a person who is detained at a police station or also elsewhere than at the police station may be photographed[602]. Where a photograph may be taken under the PACE section 64A, the only persons entitled to take the photograph are constables[603].

A photograph taken under the PACE section 64A may be used by, or disclosed to, any person for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence; and after being so used or disclosed, may be retained but may not be used or disclosed except for a purpose so related. References in the PACE section 64A to taking a photograph include references to using any process by means of which a visual image may be produced; and references to photographing a person shall be construed accordingly[604].

The legal acts of the UK do not define the persons from whom the facial images are collected from, but the procedures via which the facial images are collected, e.g. when issuing personal identification documents or within investigation procedures from detainees etc. However, for instance, it can be concluded that in accordance with PACE facial images are collected from suspect - either a person who

[601] LIVE FACIAL RECOGNITION: LEGAL MANDATE. Op.cit.
[602] Police and Criminal Evidence Act 1984. Online available: http://www.legislation.gov.uk/ukpga/1984/60/section/64A, accessed 31.10.2019.
[603] Section 64A of the Police and Criminal Evidence Act 1984.
[604] Section 64A of the Police and Criminal Evidence Act 1984.

is detained at a police station may be photographed or a person may be photographed elsewhere than at a police station[605].

One of the databases in which facial images are stored and processed is the Police National Computer (PNC), which is a national database that is available to the police sources and law enforcement authorities for which the code of practice has been developed[606] in accordance with the section 39A of Police Act 1996 (geographical extent: England and Wales)[607]. The second database PND – the Police National Database is available to all police forces and wider criminal justice agencies throughout the United Kingdom, allowing the police service to share local information and intelligence on a national basis. The PND supports delivery of three strategic benefits which are to safeguard children and vulnerable people, to counter terrorism, and to prevent and disrupt serious and organized crime[608]. There are several more databases established by each government entity in accordance with its binding rules of law also internal regulations, for example, in the field of borders, immigration and citizenship[609], the personal data of which are processed in accordance with the General Data Protection Regulation and DPA.

The facial images retained by the police are governed by the Code of Practice on the Management of Police Information and guidance set out in the College of Policing's Authorized Professional Practice.

The Protection of Freedoms Act of 2012 is an act to provide for the destruction, retention, use and other regulation of certain evidential material, which, among other things, states that the Secretary of State must prepare a code of practice containing guidance about surveillance camera systems[610]. In accordance with the Protection of Freedoms Act of 2012 section 30 the Surveillance Camera Code of Practice[611] has been issued that provides guidance on the appropriate and effective use of surveillance

[605] Section 64A of the Police and Criminal Evidence Act 1984.
[606] Code of Practice on the Operation and Use of the Police National Database. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/243554/9999102808.pdf, accessed 31.10.2019.
[607] Police Act 1996. Online available: https://www.legislation.gov.uk/ukpga/1996/16/section/39A, accessed 31.10.2019.
[608] Online available: https://www.college.police.uk/What-we-do/Learning/Professional-Training/Information-communication-technology/Pages/PND-Police-National-Database.aspx.
[609] Borders, immigration and citizenship: privacy information notice. Online available: https://www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship/borders-immigration-and-citizenship-privacy-information-notice, accessed 31.10.2019.
[610] Protection of Freedoms Act 2012. Online available: http://www.legislation.gov.uk/ukpga/2012/9/introduction/enacted, accessed 31.10.2019.
[611] This code of practice that provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities (as defined by section 33 available here: http://www.legislation.gov.uk/ukpga/2012/9/section/33/enacted) in England and Wales who must have regard to the

camera systems by relevant authorities in England and Wales who must have regard to the code when exercising any functions to which the code relates[612]. The Surveillance Camera Code of Practice provides 12 guiding principles, that system operators should adopt, for instance, that the use of a surveillance camera system must always be for a specified purpose, clearly justified, proportionate which is in pursuit of a legitimate aim. Furthermore, any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely[613].

The DPA is an act established to make provision for the regulation of the processing of information and personal data relating to individuals and for connected purposes[614]. In accordance with the DPA section 35 (1) the processing of personal data for any of the law enforcement purposes must be lawful and fair[615]. The Data Protection Act 2018 section 36 (1) states that the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected[616]. The personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed (the DPA section 37)[617].

The use of live facial recognition for law enforcement purposes constitutes 'sensitive processing' (s35 (8)(b) DPA 2018) as it involves the processing of biometric data for the purpose of uniquely identifying an individual. Sensitive processing occurs irrespective of whether that image yields a match to a person on a watchlist or the biometric data of unmatched persons is subsequently deleted within a short space of time. Such sensitive processing relates to all facial images captured and analyzed by the software; and must pay particular attention to the requirements of s35, s42 and s64 DPA 2018. As such, a Data Protection Impact Assessment (**DPIA**) and an 'appropriate policy document' must be in place. Controllers

code when exercising any functions to which the code relates. The code is applicable to various authorities. Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the code voluntarily.

[612] Protection of Freedoms Act 2012. Online available: http://www.legislation.gov.uk/ukpga/2012/9/section/30/enacted, accessed 31.10.2019.

[613] Surveillance Camera Code of Practice, June 2013. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf, accessed 31.10.2019.

[614] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted, accessed 31.10.2019.

[615] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/section/35/enacted, accessed 31.10.2019.

[616] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/section/36/enacted, accessed 31.10.2019.

[617] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/section/37/enacted, accessed 31.10.2019.

must identify a lawful basis for the use of live facial recognition. This should be identified and appropriately applied in conjunction with other available legislative instruments such as codes of practice.[618]

The legal acts of the UK do not directly determine the purposes for which it is allowed to use collected facial images. However, each government entity may specify the collection, extent, scope, use, purpose and other conditions in their internal regulations.

The laws allow the situation with regards the use of data in offence proceedings, that has been collected for other (meaning civil) purposes. However, PACE section 78 (1) determines, that in any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it[619].

In accordance with the Data Protection Act 2018 section 38 (1) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay[620]. The Data Protection Act 2018 section 39 (1) states that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed[621]. Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organizational measures (and, in this principle, "appropriate security" includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage) (the Data Protection Act 2018 section 40)[622]. Furthermore, there is established a Guide to Law Enforcement Processing for those who have day-to-day responsibility for data protection in organizations with law enforcement functions[623].

[618] Information Commissioner's Opinion. Op.cit.
[619] Police and Criminal Evidence Act 1984. Online available: http://www.legislation.gov.uk/ukpga/1984/60/section/78, accessed 31.10.2019.
[620] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/section/38/enacted, accessed 31.10.2019.
[621] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/section/39/enacted, accessed 31.10.2019.
[622] Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/section/40/enacted, accessed 31.10.2019.
[623] Guide to Law Enforcement Processing. Online available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/, accessed 03.01.2020.

The recent case of Edward Bridges vs. the Chief Constable of South Wales Police (SWP) sets out the legal precedent related to the facial recognition technology and provides the basis for the use of automated facial recognition. The case involved a member of the public who had concerns that his image may have been captured on live facial recognition technology from a police van while he was out shopping. The claimant brought the case to ask the court to decide, whether the use of live facial recognition technology in this way by the defendant was lawful. The court decided that in these circumstances it was lawful[624]. The Court considered the combination of law and practice being relied upon by SWP including, amongst other things, the police common law powers, the Surveillance Camera Code (POFA 2012), PACE and the DPA 2018 and concluded that SWP were acting in accordance with the law. In any case, law enforcement organizations will always need to articulate their lawful basis for processing in a sufficiently clear, precise and foreseeable manner to be able to justify the processing. They must do this before the processing starts. This assessment should be made by means of a DPIA and appropriate policy document as detailed at s42 DPA 2018.

Scotland

Scottish Cabinet Secretary for Justice introduced Scottish Biometrics Commissioner Bill (the Bill) in the Scottish Parliament on 30 May 2019.[625]

This will create a legal framework for the governance of present and future biometric use by Police Scotland and the Scottish criminal justice system. It is an interesting example of attempting to legislate in a way that will cope with future technical change in this area.[626]

The purpose of the Bill is to establish a new Scottish Biometrics Commissioner ("the Commissioner") who will support and promote the adoption of lawful, effective and ethical practices in relation to biometric data in a policing and criminal justice context. "Biometric data" is a relatively broad and evolving concept, encompassing "first-generation biometrics" such as fingerprints, DNA and custody photographs as well as new and emerging technologies (or "second-generation biometrics") such as

[624] Edward Bridges vs. the Chief Constable of South Wales Police. Online available: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf, accessed 03.01.2020.
[625] Online available: https://www.parliament.scot/parliamentarybusiness/Bills/111859.aspx, accessed 31.10.2019.
[626] Addendum to the 2018 Annual Report of the Biometrics Commissioner Paul Wiles, 27 June 2019. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/812362/Addendum_to_2018_BC_Report_27_06_19.pdf, accessed 31.10.2019.

facial recognition software, remote iris recognition and behavioral biometrics such as voice pattern analysis.[627]

In order to support and promote the adoption of lawful, effective and ethical practices in relation to biometric data in a policing and criminal justice context, the Commissioner will keep under review the law, policy and practice relating to the acquisition, retention, use and destruction of biometric data by specified bodies: the Police Service of Scotland ("Police Scotland") and the Scottish Police Authority ("the SPA"). The Commissioner's range of functions will include preparing and monitoring compliance with a code of practice which will provide information and guidance regarding the standards and responsibilities of Police Scotland and the SPA in relation to biometric data in order to encourage good practice, drive improvement and enhance accountability.[628]

Northern Ireland

In accordance with the Police and Criminal Evidence (Northern Ireland) Order 1989 section 64A (1) and (1A) a person who is detained at a police station or in particular case elsewhere than at a police station may be photographed. A person may be photographed if he has been arrested by a constable for an offence, taken into custody by a constable after being arrested for an offence by a person other than a constable or given a fixed penalty notice by a constable in uniform under Article 60 of the Road Traffic Offenders (Northern Ireland) Order 1996 (the Police and Criminal Evidence (Northern Ireland) Order 1989 section 64A (1B)). Where a photograph may be taken under the Police and Criminal Evidence (Northern Ireland) Order 1989 section 64A, the only persons entitled to take the photograph are constables. A photograph taken under the Police and Criminal Evidence (Northern Ireland) Order 1989 section 64A - (a) may be used by, or disclosed to, any person for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence; and (b) after being so used or disclosed, may be retained but may not be used or disclosed except for a purpose so related. References in this section 64A to taking a photograph include references to using any process by means of which a visual image may be produced; and references to photographing a person shall be construed accordingly[629].

[627] SCOTTISH BIOMETRICS COMMISSIONER BILL EXPLANATORY NOTES. Online available: https://www.parliament.scot/S5_Bills/Scottish%20Biometrics%20Commissioners%20Bill/SPBill48ENS052019.pdf, accessed 31.10.2019.
[628] Ibid.
[629] The Police and Criminal Evidence (Northern Ireland) Order 1989. Online available: http://www.legislation.gov.uk/nisi/1989/1341/article/64A, accessed 03.01.2020.

In order to clarify the use, retention, destruction etc. of biometric data the Police Service of Northern Ireland has agreed to publish a formal public policy on biometric data as part of a settlement agreement for a court case brought by the Northern Ireland Human Rights Commission[630].

Use of facial images for identity documents

The UK Visas and Immigration takes and store images in order to issue Biometric Residence Permits. Images taken for nationality purposes are then passed on to Her Majesty's Passport Office for any subsequent passport application. The Border Force compares the images of travelers using the 'ePassport Gates' to their passport photographs to help expedite passport controls. Her Majesty's Passport Office (HM Passport Office) is the authority responsible for issuing of the UK passport, that contain personal information including, but not limited to the validly digitized image (photograph)[631]. HM Passport office states that the personal data is processed under Article 6 (1) (c) and/or (e) of the General Data Protection Regulation and used for a number of purposes – customer research, training and assurance, statistical analysis, customer services messaging, images in publications and projects[632]. HM Passport Office stores the facial images of passport holders and uses them to help verify identity on every passport renewal application as well as to check against fraudulent or suspected fraudulent applications. HM Passport Office retain facial images from adult passport applications indefinitely. In accordance with the Road Traffic Act 1988 section 97 (geographical extent: England, Wales, Scotland) (1A) where any driving license to be granted to an applicant would be in the form of a photocard, the Secretary of State may in particular require him to provide a photograph which is a current likeness of him[633]. The data of the driver (also the photograph) may be shared with other government departments or public sector bodies who can demonstrate a legal power to allow it and meet the Data Protection Act requirements[634]. As stated in Road Traffic (Northern Ireland) Order 1981 section 13 (1A) an applicant is

630 Police to provide greater clarity on DNA retention in Northern Ireland. Online available: https://www.belfasttelegraph.co.uk/news/northern-ireland/police-to-provide-greater-clarity-on-dna-retention-in-northern-ireland-37694624.html, accessed 03.01.2020.

631 HM Passport Office: About us. Online available: https://www.gov.uk/government/organisations/hm-passport-office/about, accessed 31.10.2019.

632 HM Passport Office Privacy Information Notice, November 2019. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/846807/HMPO_Privacy_Information_Notice_November_2019.pdf.

633 Road Traffic Act 1988, online available: http://www.legislation.gov.uk/ukpga/1988/52/section/97?view=extent, accessed 31.10.2019.

634 Release of information from DVLA's registers. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804462/inf266-release-of-information-from-dvlas-registers.pdf, accessed 31.10.2019..

required to provide a photograph which is a current likeness of him[635]. Both authorities (HM Passport Office and Driver & Vehicle Licensing Agency) performs processing of personal data, that is governed by data protection legislation (i.e. the Data Protection Act 2018) including the General Data Protection Regulation and other relevant legislation.

Collection and use of facial images for immigration purposes

The collection and use of facial images by state (government) entity is indirectly governed by the general rules of personal data processing (i.e. the Data protection Act 2018) and the General Data Protection Regulation. However, each government entity may specify the collection, extent, scope, use, purpose and other conditions in their internal regulations.

The UK Boarders Act 2007 is an act to make provision about immigration and asylum; and for connected purposes. In accordance with the UK Boarders Act 2007 section 8 (1) the Secretary of State must by regulations make provision about the use and retention by the Secretary of State of biometric information. The regulations may include provision permitting biometric information also to be used — (a) in connection with the prevention, investigation or prosecution of an offence, (b) for a purpose which appears to the Secretary of State to be required in order to protect national security, (c) in connection with identifying persons who have died, or are suffering from illness or injury, (d) for the purpose of ascertaining whether a person has acted unlawfully, or has obtained or sought anything to which the person is not legally entitled, and (e) for such other purposes (whether in accordance with functions under an enactment or otherwise) as the regulations may specify.[636].

The Immigration (Biometric Registration) Regulations 2008 contains provisions about the use and retention of biometric information and also states that a biometric immigration document may contain the holder's facial image[637]. Photographs taken for the purposes of immigration are retained for as long as the Home Secretary considers it necessary for use in connection with an immigration or nationality function or until the person becomes a British Citizen and obtains a British passport.

[635] Road Traffic (Northern Ireland) Order 1981. Online available: http://www.legislation.gov.uk/nisi/1981/154/article/13, accessed 03.01.2020.
[636] UK Borders Act 2007. Online available: http://www.legislation.gov.uk/ukpga/2007/30/crossheading/biometric-registration, accessed 31.10.2019..
[637] The Immigration (Biometric Registration) Regulations 2008. Online available: http://www.legislation.gov.uk/uksi/2008/3048/regulation/15/made, accessed 31.10.2019.

Cross-border cooperation in offence proceedings

The binding rules of law of the UK allow the cross-border cooperation in offence proceedings by government entities, but it is subject to compliance with relevant laws, e.g. Data Protection Act 2018, part 3, chapter 5, Transfers of personal data to third countries etc.[638]. In accordance with the Data Protection Act 2018, the authority must meet certain conditions, including that the transfer is for one of the law enforcement purposes. Mostly, transfers can be undertaken to a 'relevant authority' - a body entrusted with similar law enforcement responsibilities in a third country. There are specific provisions for transfers to bodies that are not 'relevant authorities. Overall, the cross-border cooperation in offence proceedings by government entities shall be in compliance with international agreements binding on the UK and European Union legislation (subject to conditions of Brexit process).

4. ACCESS and SUBSEQUENT USE OF PERSONAL, incl. BIOMETRIC, DATA

4.1. Law enforcement' access to personal data generated by private parties

Due to the availability of data and the technological means to process them, the reuse of data is a growing trend.

Cases *Digital Rights Ireland*[639] and *Tele2 Sverige*[640] handled by the European Union Court of Justice are relevant to the scenario of law enforcement access to personal data held by private parties, as they both relate to the retention of data for later access and use by law enforcement and national securities authorities.[641]

It should be also noted that both cases were concluded before the adoption of the new data protection framework in the EU. However, the **Tele2 Sverige case was concluded after the adoption of Directive (EU) 2016/680.**

[638] Data Protection Act 2018. Online available: www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/5 , accessed 03.01.2020.
[639] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* (2014) ECLI:EU:C:2014:238.
[640] Joined cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others (2016) ECLI: EU:C:2016:970.
[641] Traffic data collected by telecoms operators for their own usage and retained to be accessed (and further used) by law enforcement authorities. The laws impose an obligation to retain the data. However, the ECJ's rulings also cover the issue of law enforcement authorities access to the retained data in addition to the issue of data retention itself.

In both cases, the ECJ had to assess whether the data retention regimes at the EU or national level constituted an interference with the right to privacy and the right to data protection and, if so, whether this interference was justified.

According to dr Jasserand-Breeman the scenario of law enforcement access to personal data generated by private parties for a non-law enforcement purpose can be split into the 'initial purpose of collection', subject to the GDPR, and the 'purpose of further processing' governed by Directive (EU) 2016/680. Law enforcement access to and use of personal data should fall into the category of data processing operations, as set out in Article 3(2) of Directive (EU) 2016/680. However, the **term 'access' is not included in the list of processing operations given as examples in Article 3(2) of Directive (EU) 2016/680.** Dr Jasserand-Breeman states that approaching the term from its terminological and operational meaning might be too simplistic to determine which legal instrument applies.[642] She also stresses that the most important thing to understand is the **purpose for which** privately held personal data are further accessed and not whether access means 'consultation' by law enforcement authorities or 'disclosure' by private parties.[643]

As for Directive (EU) 2016/680, its objective is to fight crime. However, the **ECJ found that the general objective of fighting crime is not enough to grant access to law enforcement authorities.** Access to retained data needs to be justified by the nature of the crime. **It seems that a distinction between criminal investigation and criminal intelligence is therefore necessary in relation to the nature of the criminal activity in question. However, Directive (EU) 2016/680 does not make such a distinction.** Directive (EU) 2016/680 also lacks named staff (positions) of law enforcement authorities authorised to access the personal data collected for a different purpose and also lacks categories of personal data, including biometric data, that should be accessible. [644]

In the *Digital Rights Ireland* and *Tele2 Sverige* cases, the **ECJ ruled that law enforcement access to retained personal data should be subject to prior review, either by the Court or an independent administrative body.** This procedure should be part of national criminal procedural law.[645] One might alternatively think about whether Article 28 of Directive (EU) 2016/680 provides for an oversight

[642] C. Jasserand-Breeman (2019). Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive?. Groningen, University of Groningen, p 87.
[643] C. Jasserand-Breeman (2019). Op. cit., p 88.
[644] Note: in Draft version of this Directive this provision existed. Please see: C. Jasserand-Breeman. (2019). Op. cit., p 95.
[645] Digital Rights Ireland (n 14) para 62, as complemented by Tele2 Sverige (n 15) para 120. The prior review is initiated „following a reasoned request of those authorities submitted within the procedures for the prevention, detection or prosecution of crime."

mechanism. Dr Jasserand-Breeman is of the opinion that Article 28 of Directive (EU) 2016/680 is not a sufficient procedural safeguard in that respect.[646]

In addition, based on the *Tele2 Sverige* case, **law enforcement authorities must 'notify the persons affected, as soon as possible, under the applicable national procedure'**.[647] One might alternatively think about whether Article 23 of Directive (EU) 2016/680 provides for such an obligation to notify individuals. Dr Jasserand-Breeman is of the opinion that Article 13 of Directive (EU) 2016/680 does not stipulate such an obligation.[648]

As stated above, the main issue related to data retention is **its purpose** and the main problem is the **change in the initial purpose:** what if personal data collected for a specific purpose are then reprocessed for a different purpose. Purpose limitation is 'a cornerstone of data protection'.[649] However, in situations where law enforcement authorities have access to personal data generated by private parties, the purpose of the further processing of personal data (law enforcement purpose) has no connection to the initial purpose of data collection (business or operational purpose). **Thus, the goal to process further should be deemed incompatible.** Yet, Article 4(2) of Directive (EU) 2016/680 enables the repurposing of personal data collected by other parties for a different goal **under the conditions of legality and proportionality**. Thus, there should be some sort of proper testing.

Dr Jasserand-Breeman finds it problematic that no test for compatibility in the approach of the principle of purpose limitation is set out in Directive (EU) 2016/680 itself. It is replaced by a derogation based on the principles of necessity and proportionality, which is not the same as legality and proportionality.[650]

It appears that the scenario of law enforcement access to personal data initially collected for a different purpose raises complex issues, and Directive (EU) 2016/680 lacks the essential provisions to ensure the protection of the right of individuals to data protection. If there is uncertainty surrounding the applicable rules at the EU level, then there is uncertainty surrounding interpretations at the national level, leading to the likelihood of diversions. Personal data, including biometric data, collected for a specific purpose should be used for compatible purposes or further processed under a different legal basis.

[646] C. Jasserand-Breeman. (2019). Op. cit., p 96.
[647] Tele2 Sverige (n 15) para 121.
[648] C. Jasserand-Breeman. (2019). Op. cit., p 98.
[649] Article 29 Working Party. Opinion 03/2013 on purpose limitation, (2013), WP 203, 4.
[650] C. Jasserand-Breeman. (2019). Op. cit., p 101-102.

4.2. Law enforcement's subsequent use of GDPR data

This subsection covers only the subsequent use of GDPR data by law enforcement authorities under Directive (EU) 2016/680. **It analyses the rules applicable to the reuse of GDPR data once the data have been accessed by or transferred to law enforcement authorities.**

In general, this concept relies on the **principle of purpose limitation** of personal data. The principle of purpose limitation is an element of the fundamental right to the protection of personal data,[651] and according to the ECJ, *protection against unlawful access and processing* is part of the *essence* of the fundamental right to data protection.[652] As Dr Jasserand-Breeman correctly states, any limitation to the principle of purpose limitation should comply with the conditions formulated in Article 52(1) of the Charter of Fundamental Rights.[653]

The principle of purpose limitation is sub-divided into the *principle of purpose specification* and the *principle of compatible use*.[654]

According to Article 4(1) of Directive (EU) 2016/680, personal data are *collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.* The principle is worded in identical terms in Article 5(1) of the GDPR. However, as Dr Jasserand-Breeman correctly explains, the ***principle is interpreted* differently**.[655]

According to Dr Jasserand-Breeman, **Article 4(2) of Directive (EU) 2016/680 only sets out the conditions** under which further processing for a purpose other than the original purpose of collection is allowed.[656]

The test of legality, necessity and proportionality, set out in Article 4(2) of Directive (EU) 2016/680 should be interpreted according to the case law of the Courts on Article 52(1) of the Charter and Article 8(2) of the ECHR,[657] respectively. **Since Article 4(2) of Directive (EU) 2016/680 is understood as an exception to the principle of purpose limitation, measures allowing the subsequent use of personal data**

[651] Article 8 of the Convention of Fundamental Human Rights.
[652] Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union (2017) ECLI:EU:C:2017:592, para 150.
[653] C. Jasserand-Breeman. (2019). Op. cit., p 110.
[654] Article 29 Working Party. Opinion 03/2013 on purpose limitation (2013) WP203.
[655] C. Jasserand-Breeman. (2019). Op. cit., pp 112-128.
[656] C. Jasserand-Breeman. (2019). Op. cit., p 113.
[657] C. Jasserand-Breeman. (2019). Op. cit., p 117.

should also be assessed in respect of their impact on the *essence of the fundamental right* to data protection.[658]

Article 4(2) of Directive (EU) 2016/680 does not state whether the initial purpose falls within or outside the scope of Directive (EU) 2016/680, nor does it mention the further processing of personal data.[659] **Some ambiguity exists in this Article.**

Article 19 of Directive (EU) 2016/680 sets out the accountability of law enforcement authorities to enable them to demonstrate compliance with their data protection obligations. Thus, the law enforcement authorities must comply with their data protection obligations. As Dr Jasserand-Breeman states, even if the provision itself is vague, it ties the obligation of accountability to the implementation of appropriate technical and organisational measures, such as the obligation of 'data protection by design'. This could include the adoption of policies describing the legality, necessity and proportionality assessment of the subsequent use of GDPR data and the impact on data subjects.[660]

4.3. Law enforcement's subsequent use of personal data initially collected for Directive (EU) 2016/680

One might interpret Article 4(2) of Directive (EU) 2016/680 in such a way that it applies exclusively to the further processing of personal data initially collected for one of the purposes of Directive (EU) 2016/680.

As there is a great deal of ambiguity, it appears that some of the Member States, namely the UK and the Netherlands have drafted laws to give some more clarity.

For example, both the UK and the Dutch draft laws specify the nature of the initial purpose of the collection of personal data. In the UK, Section 34 of the Data Protection Bill defines the principle of purpose limitation and restricts the rules on further processing to personal data 'collected for a law enforcement purpose'.[661] The Dutch draft law proposes a similar implementation of Article 4(2) of the

[658] C. Jasserand-Breeman. (2019). Op. cit., pp 117-118.
[659] C. Jasserand-Breeman. (2019). Op. cit., p 114.
[660] C. Jasserand-Breeman. (2019). Op. cit., pp 123-124.
[661] See Section 36 (1)- (3) of the UK Data Protection Bill, 22 online available: https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf, accessed 31 October 2019.

Directive (EU) 2016/680 since the rules on the further processing will only apply to 'police data' ('*politiegegevens*').[662]

According to Dr Jasserand-Breeman, the subsequent use of GDPR data falls within the remit of Directive (EU) 2016/680 **but is not expressly included in the scope of Article 4(2) of the Directive (EU) 2016/680.**[663]

According to Article 8 of Directive (EU) 2016/680, a processing operation is lawful if it is 'necessary for the performance of a task carried out by a competent authority' for one of the purposes of the Directive and 'is based on Union or Member State law'. **An initial processing operation is thus also subject to a legality requirement.** This requirement is understood as interpreted by the ECtHR and the CJEU, i.e. the law must be clear, accessible and foreseeable.[664]

In conclusion, the conditions of necessity and proportionality to which an initial processing operation would be subject **are not comparable** to the conditions set out in Article 4(2) of the Directive, as interpreted in Article 8 of the same Directive (EU) 2016/680. In addition, as Dr Jasserand-Breeman states, an initial processing operation **is not** subject to the requirement of 'respect of the essence of the right'.[665]

Regarding data subjects' rights, it is important to note that Article 13 of Directive (EU) 2016/680 only imposes an obligation to make specific information *available* to individuals. It does not expressly provide for an obligation to notify individuals of the processing of their personal data. However, according to the CJEU's judgment in the Tele2 Sverige[666] case, individuals whose personal data have been accessed by law enforcement authorities should be notified once the investigations are over or can no longer be jeopardised. The purpose of the notification is to allow individuals to exercise their right to remedy.[667]

As Dr Jasserand-Breeman correctly states, transparency about a possible processing operation **is not** the same as notification of an actual processing operation. One might argue that Article 13 of Directive (EU) 2016/680 should be interpreted in such a way that obliges Member States to adopt national laws to

---

662 Dutch Draft Law, Art 3, online available: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetail&qry=wetsvoorstel:34889>, accessed 31 October 2019.
663 C. Jasserand-Breeman. (2019). Op. cit., p 124.
664 Recital 33 of Directive (EU) 2016/680 with Article 8 of Directive (EU) 2016/680.
665 C. Jasserand-Breeman. (2019). Op. cit., p 126.
666 Please see n 88 in *Tele2 Sverige* case.
667 Please see n 88 para 121 in *Tele2 Sverige* case.

notify individuals of the access to and subsequent use of their personal data by law enforcement authorities.[668]

According to dr Jasserand-Breeman the absence of the obligation of notification is even less understandable in a situation where the further processing relates to individuals who are not suspects but who may be witnesses or victims in the context of a criminal investigation and even more so in the absence of any suspects in the case of criminal surveillance.[669]

Professor Kindt is of the opinion that **national law should carefully regulate** in a proportionate manner the registration, the retention and the use of such well-defined and pre-existing biometric databases held by law enforcement authorities and used for biometric identification tasks. **However, such national law framing the storage of particular biometric data is presently lacking in Member States. One of the concerns here is that these databases continuously grow and biometric data, such as facial images, are retained and used without a clear legal basis.**[670]

To conclude, **not providing a specific legal basis for the subsequent processing of GDPR data in a law enforcement context definitely creates further problems. The topic has been left in the hands of Member States and their national courts until it is challenged before the CJEU.**

4.4. Ethical considerations in live facial recognition

Law enforcement authorities around the globe have a growing appetite for personal data held by private parties and initially collected for a purpose other than law enforcement. Given their characteristics, one could consider the value of some types of personal data for law enforcement authorities. [671]

Considering the deployment of **live facial recognition** (hereinafter referred to as **LFR**) – *automated one-to-many 'matching' of near real-time video images of individuals with a curated 'watchlist' of facial images* or *other automated biometric recognition technologies* – for policing purposes, the **UK**

[668] C. Jasserand-Breeman. (2019). Op. cit., p 127.
[669] C. Jasserand-Breeman. (2019). Op. cit., p 127.
[670] About the new legal regime for biometric data. E. J. Kindt. Op.Cit.
[671] C. Jasserand-Breeman. (2019). Op. cit., p 82-83.

Biometrics and Forensics Ethics Group recommends that the following nine ethical principles be applied:[672]

1) **Public Interest:**

The use of this technology is permissible only when it is employed in the public interest. In some cases, this may be straightforward, for example, there is a public interest in being able to identify those engaged in criminal activity. Other cases may be less straightforward.

- *Why is LFR being deployed in this instance? (Crime prevention, intelligence gathering, etc.)*

2) **Effectiveness:**

The use of this technology can be justified only if it is an effective tool for identifying people.

- *How accurate is this technology? (How are false positive/negative rates calculated)?*
- *Has the LFR technology been validated using ground truth datasets?*
- *What are the criteria for successful deployment? (True positive matches/no false positive matches, increased arrests, less criminal activity/fewer arrests)?*
- *What is the quality of captured images?*
- *How is the system set up? (The importance of camera position and the network over which data are transmitted).*
- *What is the trade-off between speed and accuracy? (System features).*
- *How quickly can police officers respond to a match? (Location of the system in the field).*
- *What information do field officers receive about the match? (Is the information detailed enough to inform accurate identification and intervention)?*
- *What training do human operators have?*
- *Is human operator behaviour assessed/monitored for algorithmic deference/aversion?*
- *How is human operator error measured?*

3) **The Avoidance of Bias and Algorithmic Injustice:**

For the use of the technology to be legitimate, it should not involve or exhibit undue bias. This can be unjust in two ways. Firstly, some kinds of misrecognition are inherently demeaning and insulting. Secondly, technology with these biases can result in unequal and discriminatory treatment of some individuals (for example, members of some groups may be much more likely to be detained and/or

[672] Ethical issues arising from the police use of live facial recognition technology, interim report of the Biometrics and Forensics Ethics Group Facial Recognition Working Group, February 2019. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf, accessed 11.11.2019.

required to identify themselves). Automated biometric recognition systems (including data training sets) which will be used in public places should be open to scrutiny and effective oversight.

- *Has algorithmic bias been taken into account?*
- *How is algorithmic bias measured?*
- *What is the nature of the data in the training datasets?*

4) **Impartiality and Deployment:**

If the technology is deployed for policing purposes it must be used in an even-handed way. For example, it should not be used in ways that disproportionally target certain events, but not others, without a compelling justification.

- How are deployment sites decided?
- Who decides where LFR is deployed?
- Has a community impact assessment been undertaken?

5) **Necessity:**

Individuals normally have rights to conduct their lives without being monitored and scrutinised. Given that the use of the technology interferes with these rights, such technology can be used only if other, less invasive, techniques are not available. Furthermore, the technology should be used in ways that minimise interference with people engaging in lawful behaviour.

- What is the legal basis, if any, for the use of this technology?
- Does the watchlist include enrolled images of children?

6) **Proportionality:**

In addition to meeting a 'necessity' requirement, the technology should also meet a 'proportionality' requirement. That is, it can be permissible only if the benefits are proportionate to any loss of liberty and privacy. The benefits must be sufficiently great to justify any interference with other rights.

- What is the purpose of the deployment of LFR?
- Is the use of LFR proportionate?
- What are the costs (to individual liberty) and benefits (for public safety) of the use of LFR?
- Is the retention of captured images or data proportionate?

7) **Impartiality, Accountability, Oversight and the Construction of Watchlists:**

If humans (or algorithms) are involved in the construction of watchlists for use with the technology, it is essential that they be impartial and free from bias. The construction of 'watchlists' needs to be subject to oversight by an independent body.

- Who has oversight of these deployments?
- How will the use of LFR be evaluated?
- Who compiles the watchlist?
- How big is the watchlist?
- Why this watchlist?
- Where are enrolled images on the watchlist derived from?
- How accurate are enrolled images on the watchlist?
- What guidelines have been used for the compilation of the watchlist?
- Who has oversight of the compilation of the watchlist?
- Are any captured images or data stored?
- How long are captured images or data retained after deployment?
- Where are captured images and data stored after deployment?
- Who has access to captured images or data?
- If captured images and data are shared with other organisations, who are they shared with and why?

8) Public Trust:

If the technology is to be used for policing purposes, it is important that those using it (either in operational deployments or trials) engage in public consultation and provide the rationale for its use.

- Is LFR deployed in a trial or operational context?
- How extensively is the LFR deployment advertised in the community?
- How aware is the general public of this deployment?
- Is there adequate transparency about this deployment?
- Can members of the general public easily find out information about the deployment?
- If an oversight board has been set up, is there public representation on this board?

9) Cost-effectiveness.

Any evaluation of the use of this technology needs to take into account whether the resources it requires could be better used elsewhere.

- Is the use of LFR cost-effective?

Bibliography

1. Amnesty International, Poland: New surveillance law a major blow to human rights. Online available: https://www.amnesty.nl/actueel/poland-new-surveillance-law-a-major-blow-to-human-rights?fbclid=IwAR0_8Ypw9KgTzlRSXbMa3ATpL41dbkOSKoZF2E-J3W0UTUT6peKCp-yEsp0.

2. Baker, J. What does the newly signed 'Convention 108+' mean for UK adequacy?", 30 October 2018. Online available: https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/.

3. Biometric Update, EU Commissioner warns Malta public facial recognition plan may not meet legal requirements (08.04.2019). Available at: https://www.biometricupdate.com/201904/eu-commissioner-warns-malta-public-facial-recognition-plan-may-not-meet-legal-requirements.

4. Biometrics strategy and forensic services. Fifth Report of Session 2017–19. House of Commons Science and Technology Committee. Published on 25 May 2018. Online available: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf.

5. Closed Circuit TV. A self-contained surveillance system comprising cameras, recorders and displays for monitoring activities in a store or company. Online available: https://www.pcmag.com/encyclopedia/term/59748/cctv.

6. Council of Europe. Practical guide on the use of personal data in the police sector, Strasbourg, 15 February 2018 T-PD(2018)01. Online available: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

7. Demetriou, C. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Cyprus (01.07.2016), FRANET contractor: University of Nicosia and Symfiliosi. Online available at: https://fra.europa.eu/sites/default/files/fra_uploads/cyprus-study-data-surveillance-ii-cy.pdf.

8. European Union Agency For Fundamental Rights. FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement. 27 November 2019. Online available: https://fra.europa.eu/en/publication/2019/facial-recognition.

9. Flaherty, D. On the Utility of Constitutional Rights to Privacy and Data Protection. Case W. Res. L.Rev., 1990-1991.
10. Freedom House, Polish Government Expands Power to Monitor Citizens, Block Internet. Available at: https://freedomhouse.org/article/polish-government-expands-power-monitor-

citizens-block-internet?fbclid=IwAR3aRQzr1k8q-TDOsiAIhIkpoWOyP8_UxyHdaRRtnyzTcI_mni0E3b8vE_U.

11. Gesley, J. Germany: Federal Constitutional Court Declares Terrorism Legislation Partially Unconstitutional, Global Legal Monitor (May 3, 2016), http://www.loc.gov/law/foreign-news/article/germany-federal-constitutional-court-declares-terrorism-legislation-partially-unconstitutional/, *archived at* http://perma.cc/HEM5-JBC8.

12. Grout, V. No More Privacy Any More? Published 01 January 2019. Online available: https://www.mdpi.com/2078-2489/10/1/19/htm.

13. Habib, K. Malta: UN expert recommends broad changes to surveillance laws, GENEVA (18 December 2019). Available at: https://unric.org/it/malta-un-expert-recommends-broad-changes-to-surveillance-laws/.

14. Handbook on European data protection law 2018 edition. Online available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

15. Hudson, D. Police surveillance during protests may be unlawful, IT Law association says (04.12.2019). Available at: https://www.maltatoday.com.mt/news/national/99057/police_surveillance_during_protests_may_be_unlawful_it_law_association_says#.Xg4Nfi2ZNQI.

16. Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places, 31.10.2019. Online available: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

17. Jasserand-Breeman, C. (2019). Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between GDPR and the "Police" directive? Groningen, University of Groningen.

18. Kindt, E. J. Computer Law and Security Review Volume 34, Issue 3, June 2018. Having yes, using no? About the new legal regime for biometric data., pp 523-538.

19. Kindt, E. J. Doctoral thesis 'The processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a Legal framework', Katholieke Univerisiteit Leuven 2012. Online available: https://lirias.kuleuven.be/bitstream/123456789/345184/1/PH_D_text_PartI%2BPartII_17.04-Pservice.pdf.
20. Kindt, E. J. Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis. Springer, 2013, 975 pages.

21. Misra, P. (2018). Here's how face recognition tech can be GDPR compliant. Online available: https://thenextweb.com/contributors/2018/10/29/heres-how-face-recognition-tech-can-be-gdpr-compliant/.

22. Pajunoja, L. J. The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU's data protection law and its compatibility with the right to privacy. University of Helsinki, Faculty of Law, 2017.

23. Pascu, L. Veridos to upgrade Cyprus biometric passport and data collection system (26.11.2019), available at: https://www.biometricupdate.com/201911/veridos-to-upgrade-cyprus-biometric-passport-and-data-collection-system.

24. Pavlou, S., Nicolaou, C., Philippidou, K. and Siopacha, G. Litigation and enforcement in Cyprus. Patrikios Pavlou & Associates LLC, available at: https://uk.practicallaw.thomsonreuters.com/7-502-0202?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

25. Siseministeerium, Biomeetriliste andmete kasutamise kontseptsioon. Online available: https://adr.siseministeerium.ee/sisemin/dokument/907446.

26. Vainio, N. Fundamental rights Compliance and the politics of interpretation: Explaining Member State and court reactions to Digital Rights Ireland. T. Bräutigam & S. Miettinen, Data Protection, Privacy and European Regulation in the Digital Age, p 229-260. Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, 2016.

27. Watson, G. EC drafting laws to rein in Facial Recognition Technology (23.08.2019). Available at: https://newsbook.com.mt/en/ec-drafting-laws-reigning-in-facial-recognition-technology/.

28. Zammit, F. 'Safe City Malta': Is Privacy the Real Crux of the Matter? (16.01.2019). Available at: https://www.islesoftheleft.org/safe-city-malta-is-privacy-the-real-crux-of-the-matter/.

List of Normative Acts and Explanatory Reports

1. 101/1998. (V. 22.) Korm. rendelet a külföldre utazásról szóló 1998. évi XII. törvény végrehajtásáról, published 1998. Online available: https://net.jogtar.hu/jogszabaly?docid=99800101.KOR.

2. 16/2014. (XII. 19.) IM rendelet a szabadságvesztés, az elzárás, az előzetes letartóztatás és a rendbírság helyébe lépő elzárás végrehajtásának részletes szabályairól, published 2014. Online available: https://net.jogtar.hu/jogszabaly?docid=a1400016.im.

3. 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról, published 1992. Online available: https://net.jogtar.hu/jogszabaly?docid=99200066.TV.

4. 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről, published 1996. Online available: https://net.jogtar.hu/jogszabaly?docid=99600038.TV.

5. 1998. évi XII. törvény a külföldre utazásról, published 1998. Online available: https://net.jogtar.hu/jogszabaly?docid=99800012.TV.

6. 1999. évi LXXXIV. törvény a közúti közlekedési nyilvántartásról, published 1999. Online available: https://net.jogtar.hu/jogszabaly?docid=99900084.TV.

7. 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, entry into force 30.06.2009. Online available: https://net.jogtar.hu/jogszabaly?docid=A0900047.TV.

8. 2012. évi C. törvény a büntető törvénykönyvről, entry into force 01.07.2013. Online available: https://net.jogtar.hu/jogszabaly?docid=A1200100.TV.

9. 2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről, entry into force 15.04.2012. Online available: https://net.jogtar.hu/jogszabaly?docid=A1200002.TV.

10. 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról, entry into force 01.01.2015. Online available: https://net.jogtar.hu/jogszabaly?docid=A1300240.TV#lbj0id899a.

11. 2013. évi LXXXVIII. törvény a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról, published 2013. Online available: https://net.jogtar.hu/jogszabaly?docid=A1300088.TV.

12. 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről, published 2015. Online available: https://net.jogtar.hu/jogszabaly?docid=A1500188.TV.

13. 2017. évi XC. Törvény a büntetőeljárásról, entry into force: 01.07.2018. Online available: https://net.jogtar.hu/jogszabaly?docid=A1700090.TV.

14. 326/2011. (XII. 28.) Korm. rendelet a közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról, entry into force 01.01.2012. Online available: https://net.jogtar.hu/jogszabaly?docid=A1100326.KOR.

15. 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól, published 2015. Online available: https://net.jogtar.hu/jogszabaly?docid=A1500414.KOR.

16. Aanwijzing technisch opsporingsonderzoek/deskundigenonderzoek, valid from 01.06.2013. Online available: https://wetten.overheid.nl/BWBR0033475/2013-06-01.

17. Aliens Act, entry into force 01.10.2010, online available: https://www.riigiteataja.ee/en/eli/ee/529032019002/consolide/current.

18. Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin, entry into force 9.08.2006, online available: http://gesetze.berlin.de/jportal/;jsessionid=68E784CA5AEF8FDB51E21B42DF30A4BA.jp26?quelle=jlink&query=ASOG+BE&psml=bsbeprod.psml&max=true&aiz=true#jlr-ASOGBE2006pP18.

19. Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, WP 193, Brussels, 27 April 2012.

20. Article 29 Working Party. Opinion 03/2013 on purpose limitation, (2013), WP 203, 4.

21. Article 68(b) of the Police Act. Available at: https://www.legislationline.org/download/id/1010/file/bbf10ad5a4cc4633a8f3779af9001b20.pdf.

22. Basiswet betreffende het gevangeniswezen en de rechtspositie van de gedetineerden 2005, online available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2005011239.

23. Baudžiamojo proceso kodeksas, entry into force 01.05.2003. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr.

24. Bausmių vykdymo kodeksas, entry into force 19.07.2002. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.171368/asr.

25. Bekendtgørelse af lov om fuldbyrdelse af straf m.v., entry into force 01/07/2001. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=194713.

26. Bekendtgørelse af lov om rettens pleje, entry into force 01.01.1961. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=202196.

27. Bekendtgørelse af udlændingeloven, entry into force 01.10.1983. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=208100.

28. Bekendtgørelse om fotografering og optagelse af fingeraftryk af indsatte i kriminalforsorgens institutioner (fotobekendtgørelsen), entry into force 30.01.2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=206605.

29. Bekendtgørelse om kørekort, entry into force 27.08.2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=210058.

30. Bekendtgørelse om ophold i varetægt, entry into force: 01.02.2019. Online available: https://www.retsinformation.dk/Forms/R0710.aspx?id=206603.

31. Bekendtgørelse om pas m.v.), entry into force 01.12.2013. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=159226.

32. Besluit identiteitsvaststelling verdachten en veroordeelden, valid from 01.06.2016. Online available: https://wetten.overheid.nl/BWBR0026302/2016-06-01.

33. Borders, immigration and citizenship: privacy information notice. Online available: https://www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship/borders-immigration-and-citizenship-privacy-information-notice.

34. Brottsdatalag 2018:1177, entry into force 01.08.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177.

35. BSI-Standard 100-1, Information Security Management Systems, online available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1.

36. Bundesdatenschutzgesetz, entry into force 30.06.2017, online available: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html.

37. Bundesregierung [Federal Government], Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus /Draft Act of the Federal Government, Draft Act to Introduce Improved Information Sharing for the Fight Against International Terrorism*]*, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/entw-infoaustausch-terrorbek.pdf;jsessionid=8F0CDB27679238C6F4A52F3143693585.2_cid287?__blob=publicationFile, *archived at* http://perma.cc/2WPG-4GV8.

38. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 100 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] [Decisions of the Federal Constitutional Court] 313, 366 *et seq.*, http://www.bundesverfassungsgericht.de/ SharedDocs/Entscheidungen/EN/1999/07/rs19990714_1bvr 222694en.html.

39. Civil Registry Law 2002, online available: http://www.cylaw.org/nomoi/enop/non-ind/2002_1_141/full.html.

40. Code de procédure pénale, consolidated version 24.08.2019. Online available: http://data.legilux.public.lu/file/eli-etat-leg-code-procedure_penale-2019-08-24-fr-pdf.pdf.

41. Code of Criminal Procedure, entry into force 01.07.2004, online available: https://www.riigiteataja.ee/en/eli/ee/508042019008/consolide/current.

42. Code of Criminal Procedure, entry into force 01/01/1962, online available: https://www.legislationline.org/download/id/6371/file/Czech%20Republic_CPC_1961_am2012_en.pdf.

43. Code of Misdemeanour Procedure, entry into force 01.09.2002, online available: https://www.riigiteataja.ee/en/eli/508042019014/consolide.

44. Code of Practice on the Operation and Use of the Police National Database. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/243554/9999102808.pdf.

45. Codice di procedura penale, entry into force 24/10/1989. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447.

46. Codice Penale, entry into force 01/07/1931. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1930-10-19;1398.

47. CODUL DE PROCEDURĂ PENALĂ, published 15.07.2010. Online available: http://legislatie.just.ro/Public/DetaliiDocument/120611.

48. Constitución Española, entry into force 29.12.1978, online available: https://www.boe.es/eli/es/c/1978/12/27/(1)/con.

49. Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed by the contracting parties in Prüm (Germany) on 27 May 2005. Online available: https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/prumtr.pdf.

50. Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 04 November 1950. Online available: https://www.echr.coe.int/Documents/Convention_ENG.pdf.

51. Convention for the protection of individuals with regard to the processing of personal data. Online available: http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

52. Convention on Cybercrime, Budapest, 23 November 2001 (European Treaty Series - No. 185) Online available: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000001680081561.

53. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (2008) OJ L210/1 (PRÜM Decision). Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615.

54. COUNCIL DECISION 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Online available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0533.

55. COUNCIL DECISION 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. Online available: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejdecision/Consolidated%20version%20of%20the%20Eurojust%20Council%20Decision/Eurojust-Council-Decision-2009Consolidated-EN.pdf.

56. COUNCIL FRAMEWORK DECISION 2006/960/JH of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960.

57. COUNCIL OF EUROPE COMMITTEE OF MINISTERS RECOMMENDATION No. R (87) 15 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR, 17 September 1987. Online available: https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_87_15.pdf.

58. Criminal Code 1854. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574&l=1.

59. Criminal Justice (Forensic Evidence and DNA Database System) Act no 11 of 2014. Online available: http://www.irishstatutebook.ie/eli/2014/act/11/enacted/en/pdf.

60. Cyprus, Law amending the law on protection of confidentiality of private communication (Surveillance of conversations) and access to registered content of private communication of 1996, available at http://cylaw.org/nomoi/arith/2015_1_216.pdf.

61. Cyprus, Law on the processing of personal data (Protection of the individual) of 2001. Available at http://cylaw.org/nomoi/enop/non-ind/2001_1_138/full.html.

62. Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών) N. 75(I)/2016, articles 4 and 5(2), available at www.cylaw.org/nomoi/arith/2016_1_075.pdf.

63. Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service, available at www.cylaw.org/nomoi/arith/2016_1_075.pdf.

64. Data Protection Act 2018. Online available: http://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted.

65. Data Protection Act no 7 of 2018. Online available: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/pdf.

66. DATA PROTECTION (PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE PURPOSES OF THE PREVENTION, INVESTIGATION, DETECTION OR PROSECUTION OF CRIMINAL OFFENCES OR THE EXECUTION OF CRIMINAL PENALTIES) REGULATIONS 2018. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12840&l=1.

67. Datenschutzgesetz, entry into force 01/01/2000, online available: https://www.ris.bka.gv.at/Dokumente/BgblPdf/1999_165_1/1999_165_1.pdf.

68. Decree no. 2019-452 of 13 May 2019 authorising the creation of an electronic identification method called "Authentification en ligne certifiée sur mobile" (Mobile-Based Certified Online Authentication: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= JORFTEXT000038475477&categorieLien=id.

69. DECRETO-LEGGE n. 59 Norme penali e processuali per la prevenzione e la repressione di gravi reati, 21/03/1978. Online available: https://www.gazzettaufficiale.it/eli/id/1978/03/22/078U0059/sg.

70. Dėl Motorinių transporto priemonių vairuotojo pažymėjimų išdavimo taisyklių patvirtinimo, entry into force 17.09.2008. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.327050/asr.

71. Dėl nuotraukų asmens dokumentams reikalavimų patvirtinimo, entry into force 01.01.2003. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.197394/asr.

72. Den svenska rättegångsbalken. SFS 1942:740, entry into force 01/01/1948. Online available: https://www.government.se/49e41c/contentassets/a1be9e99a5c64d1bb93a96ce5d517e9c/the-swedish-code-of-judicial-procedure-ds-1998_65.pdf.

73. DETENTION SERVICE REGULATIONS 2016. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12538&l=1.

74. DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

75. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. No longer in force, Date of end of validity: 24/05/2018. Latest consolidated version 20/11/2003 online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01995L0046-20031120.

76. Dutch Draft Law, Art 3, online available: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetail&qry=wetsvoorstel:34889>.

77. Employment Permits Regulations no 95 of 2017. Online available: http://www.irishstatutebook.ie/eli/2017/si/95/made/en/pdf.

78. Equality Act 2010. Online available: http://www.legislation.gov.uk/ukpga/2010/15/contents.

79. European Arrest Warrant (Application to Third Countries and Amendment) and Extradition (Amendment) Act no 30 of 2012. Online available: http://www.irishstatutebook.ie/eli/2012/act/30/enacted/en/pdf.

80. European Commission Impact Assessment Report on the establishment of an EU Entry Exit System. Brussels, 6.4.2016. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0115&qid=1573980037866&from=EN.

81. Europol – Malta, available at: https://www.europol.europa.eu/partners-agreements/member-states/malta.
82. Europol Act no 53 of 2012. Online available: http://www.irishstatutebook.ie/eli/2012/act/53/enacted/en/pdf.

83. Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223 Strasbourg, 10.X.2018. Online available: https://rm.coe.int/16808ac91a.

84. Fotografie da apporre sulla patente di guida, 20/10/2016. Online available: http://www.patente.it/normativa/circolare-20-10-2016-n-23176-foto-per-patente?idc=3366.

85. Fremdenpolizeigesetz, entry into force 01/01/2006, online available: https://tinyurl.com/y688oh6x.

86. Förordning (1992:824) om fingeravtryck m.m., entry into force 01.08.1992. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-1992824-om-fingeravtryck-mm_sfs-1992-824.

87. Förordning 2005:661 om nationellt identitetskort, entry into force 01.10.2005. Online available: http://rkrattsbaser.gov.se/sfst?bet=2005:661.

88. Förordning 2018:219 med kompletterande bestämmelser till EU:s dataskyddsförordning, entry into force 25.05.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219.

89. Führerscheingesetz, entry into force 01/11/1997, online available: https://tinyurl.com/yyzpzyv7.

90. GARDA SÍOCHÁNA ACT no 20 of 2005. Online available: http://www.irishstatutebook.ie/eli/2005/act/20/enacted/en/pdf.

91. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel 10-Gesetz] [G 10] [Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications] [Article 10 Act], June 26, 2001, BGBl. I at 1254, 2298, as amended, http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf.

92. Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, entry into force 1.06.2017, online available: http://www.gesetze-im-internet.de/bkag_2018/BJNR135410017.html.

93. Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung, entry into force 16.03.1976, online available https://www.gesetze-im-internet.de/stvollzg/BJNR005810976.html.

94. Gesetz über die Bundespolizei, entry into force 19.10.1994, online available: https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html.

95. Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz), entry into force 20.12.1990, online available: https://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html.

96. *Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus* [*Draft Act of the Federal Government, Draft Act to Introduce Improved Information Sharing for the Fight Against International Terrorism*], https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/entw-infoaustausch-terrorbek.pdf;jsessionid=8F0CDB27679238C6F4A52F3143693585.2_cid287?__blob=publicationFile.

97. HM Passport Office Privacy Information Notice, November 2019. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/846807/HMPO_Privacy_Information_Notice_November_2019.pdf.

98. HOTĂRÂRE nr. 556/2006 privind stabilirea datei de la care se eliberează pa□apoarte simple temporare, precum □i a formei □i con□inutului acestora, published 02.05.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocument/71142.

99. HOTĂRÂRE nr. 557/2006 privind stabilirea datei de la care se pun în circula□ie pa□apoartele electronice, precum □i a formei □i con□inutului acestora, published 02.05.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocument/71143.

100. HOTĂRÂRE nr. 801 din 26 octombrie 2016 pentru stabilirea procedurilor de colectare şi ştergere a datelor persoanelor cu identitate declarată, precum şi pentru modificarea şi completarea unor acte normative privind aplicarea unitară a dispozițiilor în materie de stare civilă şi evidența persoanelor, published 03.11.2016. Online available: http://legislatie.just.ro/Public/DetaliiDocument/183323.

101. Human Rights Act 1998. Online available: http://www.legislation.gov.uk/ukpga/1998/42/contents.

102. IDENTITY CARD AND OTHER IDENTITY DOCUMENTS ACT 2012. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8751&l=1.

103. Identity Documents Act, entry into force 01.01.2000, online available: https://www.riigiteataja.ee/en/eli/529032019005/consolide.

104. Immigration Act no 1 of 2004. Online available: http://www.irishstatutebook.ie/eli/2004/act/1/enacted/en/pdf.

105. Imprisonment Act, entry into force 01.12.2000, online available: https://www.riigiteataja.ee/en/eli/ee/520062019002/consolide/current.

106. Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196, 24/05/2017. Online available: https://www.gazzettaufficiale.it/eli/gu/2017/06/24/145/so/33/sg/pdf.

107. Kamerabevakningslag 2018:1200, entry into force 01/08/2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200.

108. Kazneni zakon, effective from 04.01.2019, online available: https://www.zakon.hr/z/98/Kazneni-zakon.

109. Kodeks karny wykonawczy, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970900557.

110. Kodeks karny, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970880553.

111. Kodeks postępowania karnego, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555.

112. Kodeks postępowania karnego, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555.

113. Kodeks postępowania karnego, entry into force 01.09.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555.

114. Kodeks pracy, entry into force 01.01.1975, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19740240141.

115.

116. KOMENDA GŁÓWNA POLICJI, The Right of Data Subjects to Information, available at: http://www.policja.pl/pol/sirene/prawo-osob-do-informac/76188,The-right-of-data-subjects-to-information.html.

117. Koninklijk besluit betreffende de identiteitskaarten 2003, online available: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2003032531&table_name=wet.

118. Koninklijk besluit betreffende het rijbewijs 1998, online available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1998032331&table_name=wet.

119. Körkortslag 1998:488, entry into force 01.10.1998. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/korkortslag-1998488_sfs-1998-488.

120. Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, entry into force 01/01/2019. Online available: http://rkrattsbaser.gov.se/sfst?bet=2018:1693.

121. Lag 1964:167 med särskilda bestämmelser om unga lagöverträdare, issued 20.03.1964. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-1964167-med-sarskilda-bestammelser-om-unga_sfs-1964-167.

122. Lag 2003:389 om elektronisk kommunikation, entry into force 25.07.2003. Online available: http://rkrattsbaser.gov.se/sfst?bet=2003:389.

123. Lag 2012:278 om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, entry into force 01.07.2012. Online available: http://rkrattsbaser.gov.se/sfst?bet=2012:278.

124. Lag 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning, entry into force 25.05.2018. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218.

125. Laki henkilötietojen käsittelystä poliisitoimessa, entry into force 01.06.2019, online available: http://www.finlex.fi/fi/laki/alkup/2019/20190616?search%5Btype%5D=pika&search%5Bpika%5D=616%2F2019#Pidp447484848.

126. Law 125(I)/2018, available at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3b_en/page3b_en?opendocument.

127. Law 2(III) of 2000 on Mutual Assistance in Criminal Matters, available at: http://www.cylaw.org/nomoi/arith/2000_3_002.pdf.

128. Law 2(III) of 2000 on mutual assistance in criminal matters, online available: http://www.cylaw.org/nomoi/arith/2000_3_002.pdf.

129. Law 20 (III) of 2000 ratifying the European convention on criminal procedures, available at: http://www.cylaw.org/nomoi/arith/2000_3_002.pdf.

130. Law 23(I)/2001 on International Co-operation on Criminal Matters, online available: http://www.cylaw.org/nomoi/indexes/2001_1_23.html.

131. Law 23(I)/2001 on International Co-operation on Criminal Matters, available at: http://www.cylaw.org/nomoi/indexes/2001_1_23.html.

132. Law 44(I)/2019, available at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/A5C70C14703B857DC225820A004B5CA0/$file/Law%202019_1_044.pdf.

133. Law Enforcement Act, entry into force 01.07.2014, online available: https://www.riigiteataja.ee/en/eli/525032019010/consolide.

134. Law n ° 78-17 of January 6, 1978 relating to data processing, files and freedoms. https://www.cnil.fr/fr/la-loi-informatique-et-libertes.

135. Law no 2472/1997 of Greek Republic on the Protection of Individuals with regard to the Processing of Personal Data, published 10/04/1997. Online available: http://tiny.cc/upindz.

136. Law no 2776/1999 of Greek Republic, published 24/12/1999. Online available: http://www.et.gr/index.php/nomoi-proedrika-diatagmata.

137. Law no 4624/2019 of the Greek Republic, published 29.08.2019. Online available: http://tiny.cc/hkindz.

138. Law on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data 2019, online available: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/A5C70C14703B857DC225820A004B5CA0/$file/Law%202019_1_044.pdf.

139. Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data, 31/07/2018, online available: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3b_en/page3b_en?opendocument.

140. Legal systems in the UK: overview, by Professor Suzanne Rab, Serle Court, Dec 2019. Online available: https://uk.practicallaw.thomsonreuters.com/5-636-2498?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

141. Lege nr. 118/2019 privind Registrul na□ional automatizat cu privire la persoanele care au comis infrac□iuni sexuale, de exploatare a unor persoane sau asupra minorilor, precum □i pentru completarea Legii nr. 76/2008 privind organizarea □i func□ionarea Sistemului Na□ional de Date Genetice Judiciar, published 26.06.2019. Online available: http://legislatie.just.ro/Public/DetaliiDocument/215496.

142. LEGE nr. 218/2002 privind organizarea □i func□ionarea Poli□iei Române, published 25/04/2014. Online available: http://legislatie.just.ro/Public/DetaliiDocument/35841.

143. Lege nr. 248/2005 privind regimul liberei circula□ii a cetățenilor români în străinătate, published 29.07.2005. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/63704.

144. Lege nr. 254/2013 privind executarea pedepselor □i a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal, published 14.08.2013. Online available: http://legislatie.just.ro/Public/DetaliiDocument/150699.

145. LEGE nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracțiunilor sau al executării pedepselor, măsurilor educative şi de siguranță, precum şi privind libera circulație a acestor date, entry into force 10.01.2019. Online available: http://legislatie.just.ro/Public/DetaliiDocument/209627.

146. Legea nr. 286/2009 Codul Penal, published 24.07.2009. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/210277.

147. Legge 21 novembre 1967, n. 1185 (1). Norme sui passaporti (1/a) (1/circ)), 21/11/1967. Online available: https://www.esteri.it/mae/doc/l1185_1967.pdf.

148. Leggi di pubblica sicurezza, entry into force 11/07/1931. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1931-06-18;773!vig=.

149. Ley de Seguridad Privada, entry into force 05.06.2014, online available: https://www.boe.es/eli/es/l/2014/04/04/5/con.

150. Ley de transparencia, acceso a la información pública y buen gobierno, entry into force 10.12.2014, online available: https://www.boe.es/eli/es/l/2013/12/09/19/con.

151. Ley del Procedimiento Administrativo Común de las Administraciones Públicas, entry into force 02.10.2016, online available: https://www.boe.es/eli/es/l/2015/10/01/39/con.

152. Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, entry into force 07/12/2018, online available: https://www.boe.es/eli/es/lo/2018/12/05/3/con.

153. Ley Orgánica de protección de la seguridad ciudadana, entry into force 01.07.2015, online available: https://www.boe.es/eli/es/lo/2015/03/30/4/con.

154. Ley Orgánica del Código Penal, entry into force 24/05/1996, online available: https://www.boe.es/eli/es/lo/1995/11/23/10/con.

155. Ley Orgánica por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, entry into force 06.08.1997, online available: https://www.boe.es/eli/es/lo/1997/08/04/4/con.

156. Ley Orgánica reguladora de la responsabilidad penal de los menores, entry into force 13.01.2001, online available: https://www.boe.es/eli/es/lo/2000/01/12/5/con.

157. Ley por la que se establecen medidas para la protección de las infraestructuras críticas, entry into force 30/04/2011, online available: https://www.boe.es/eli/es/l/2011/04/28/8/con.

158. Ley sobre reutilización de la información del sector público, entry into force 17.01.2008, online available: https://www.boe.es/eli/es/l/2007/11/16/37/con.

159. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas, entry into force 01.07.2011. Online available: https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr.

160. Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas, entry into force 02.03.2015. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f26839f08f5011e48028e9b85331c55d/asr.

161. Lietuvos Respublikos finansinių nusikaltimų tyrimo tarnybos įstatymas, entry into force 01.04.2002. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163326.

162. Lietuvos Respublikos įstatymas dėl užsieniečių teisinės padėties, entry into force 30.04.2004. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232378/asr.

163. Lietuvos Respublikos kriminalinės žvalgybos įstatymas, entry into force 01.01.2013. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.434526/asr.

164. Lietuvos Respublikos policijos įstatymas, entry into force 27.10.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111665/asr.

165. Lietuvos Respublikos prokuratūros įstatymas, entry into force 01.01.1995. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.5956/asr.

166. Lietuvos Respublikos specialiųjų tyrimų tarnybos įstatymas, entry into force 01.06.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.100816/asr.

167. Lietuvos Respublikos žvalgybos įstatymas, entry into force 31.07.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/asr.

168. Lietuvos Respublikos tarnybinio paso įstatymas, entry into force 26.01.2000. Online available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.94414/asr.

169. LIVE FACIAL RECOGNITION: LEGAL MANDATE, version 1-01. Online available: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/mps-lfr-legal-mandate-v1-1.pdf.

170. Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques. Online available: http://data.legilux.public.lu/file/eli-etat-leg-memorial-2013-107-fr-pdf.pdf.

171. Lov om retshåndhævende myndigheders behandling af personoplysninger, entry into force: 2017. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=189891.

172. Lov om udstedelse af legitimationskort, entry into force 01.07.2017. Online available: https://www.retsinformation.dk/Forms/r0710.aspx?id=187037.

173. Malta, House of Representatives (1996), Security Service Act, 26 July 1996, 6 September 1996, available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8858&l=1.

174. Malta, House of Representatives (2013), Processing of Personal Data (Electronic Communications Sector) (Amendment) Regulations, 2013, 1 January 2013, available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=25839&l=1.

175. METODOLOGIE din 26 ianuarie 2011 cu privire la aplicarea unitară a dispozi□iilor în materie de stare civilă, published 02/03/2011. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/220201.

176. Ministerial Decision 3021/22/2005, published 06.07.2005. Online availble: http://www.passport.gov.gr/en/downloads/nomothetiko-plaisio/11.html.

177. Ministerial Decision no. 3021/ published 18/10/2005. Online available: https://www.e-nomothesia.gr/kat-deltia-tautotetos/kya-3021-19-53-2005.html.

178. Ministerial Decision no. 50984/7947/2013, published 02.12.2003. Online available: https://www.e-nomothesia.gr/kat-aytokinita/adeies-odegeses/ya-a3-oik-50984-7947-2013.html.

179. Ministerial Decree no. 51/2012, published 27/4/2012. Online available: https://www.e-nomothesia.gr/kat-aytokinita/adeies-odegeses/pd-51-2012.html.

180. MOTOR VEHICLES REGULATIONS 1994. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=9196&l=1.

181. НАКАЗАТЕЛНО-ПРОЦЕСУАЛЕН КОДЕКС, entry into force 29.04.2006, online available: https://www.lex.bg/bg/laws/ldoc/2135512224.

182. Niederlassungs- und Aufenthaltsgesetz, entry into force 01/01/2006, online available: https://tinyurl.com/y3shnun9.

183. NORME METODOLOGICE de aplicare a Legii nr. 248/2005 privind regimul liberei circula□ii a cetă□enilor români în străinătate, published 27.01.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/205565.

184. NORME METODOLOGICE de aplicare unitară a dispozi□iilor legale privind eviden□a, domiciliul, re□edin□a □i actele de identitate ale cetă□enilor români, published 17.10.2006. Online available: http://legislatie.just.ro/Public/DetaliiDocumentAfis/188152.

185. Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012, given by The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, online available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

186. Opinion of the CNIL: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038475742.

187. Opinion of the Italian Data Protection Authority on Automatic system for searching the identity of a face, 26/07/2018. Online available: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256.

188. ORDIN nr. 97/2017 privind procedura □i condi□iile tehnice în care se realizează □i se stochează înregistrările examenului de ob□inere a permisului de conducere □i măsurile pentru protejarea acestora □i a datelor cu caracter personal, published 19.08.2017. Online available: http://legislatie.just.ro/Public/DetaliiDocument/192464.

189. Paspoortwet, valid from 01.10.2017. Online available: https://wetten.overheid.nl/BWBR0005212/2017-10-01.

190. Passförordning 1979:664, issued 28.06.1979. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/passforordning-1979664_sfs-1979-664.

191. Passgesetz, entry into force 01/01/1993, online available: https://tinyurl.com/y4gwcfh5.

192. Passgesetz, entry into force 19.04.1986, online available: http://www.gesetze-im-internet.de/pa_g_1986/BJNR105370986.html.

193. Passlag 1978:302, issued 25.05.1978. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/passlag-1978302_sfs-1978-302.

194. Passports Act no 4 of 2008. Online available: http://www.irishstatutebook.ie/eli/2008/act/4/enacted/en/pdf.

195. PASSPORT REGULATIONS 1993. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=9184&l=1.

196. Personalausweisgesetz, entry into force 18.06.2009, online available: https://www.gesetze-im-internet.de/pauswg/BJNR134610009.html.

197. Police Act 2017. Online available: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8686&l=1.

198. Police Act 1996. Online available: https://www.legislation.gov.uk/ukpga/1996/16/section/39A.

199. Police Act, entry into force 21/06/1991, online available: https://www.legislationline.org/download/id/1020/file/087ab6b8f317a8515e647ae55747.pdf.

200. Police and Criminal Evidence Act 1984. Online available: http://www.legislation.gov.uk/ukpga/1984/60/section/64A.

201. Polisdatalag 2010:361, entry into force 01.03.2012. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/polisdatalag-2010361_sfs-2010-361.

202. Pravilnik o načinu postupanja policijskih službenika, effective from 19.07.2010, online available: https://narodne-novine.nn.hr/clanci/sluzbeni/2010_07_89_2528.html.

203. PRAVILNIK O OBLIKU I SADRŽAJU IDENTIFIKACIJSKE VOJNE ISKAZNICE, effective from 2014, online available: http://www.propisi.hr/print.php?id=9147.

204. PRAVILNIK O PRIJAMU I POSTUPANJU S UHIĆENIKOM I PRITVORENIKOM TE O EVIDENCIJI PRITVORENIKA U PRITVORSKOJ POLICIJSKOJ JEDINICI, effective from 2019, online available: http://www.propisi.hr/print.php?id=9465.

205. PRAVILNIK O VOZAČKIM DOZVOLAMA, effective from 2019, online available: http://www.propisi.hr/print.php?id=7651%20.

206. ПРАВИЛНИК ЗА ПРИЛАГАНЕ НА ЗАКОНА ЗА ИЗПЪЛНЕНИЕ НА НАКАЗАНИЯТА И ЗАДЪРЖАНЕТО ПОД СТРАЖА 2010, online available: https://www.lex.bg/laws/ldoc/2135661301.

207. Prawo prasowe, entry into force 01.07.1984. online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19840050024.

208. ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ 'ΑΡΙΘΜ. 178 Οργανισμός Υπηρεσιών Ελληνικής Αστυνομίας, published 31/12/2014. Online available: https://www.e-nomothesia.gr/kat-astynomikos-astynomia/idrysi-leitourgia-uperesion/pd-178-2014.html.

209. Protection of Freedoms Act 2012. Online available: http://www.legislation.gov.uk/ukpga/2012/9/introduction/enacted.

210. Real Decreto de por el que se aprueba la Ley de Enjuiciamiento Criminal, entry into force 03.01.1883, online available: https://www.boe.es/eli/es/rd/1882/09/14/(1)/con.

211. Real Decreto Legislativo por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, entry into force 31.01.2016, online available: https://www.boe.es/eli/es/rdlg/2015/10/30/6/con.

212. Real Decreto por el que se aprueba el Reglamento General de Conductores, entry into force 08/12/2009, onlibe available: https://www.boe.es/eli/es/rd/2009/05/08/818/con.

213. REAL DECRETO POR EL QUE SE REGULA LA EXPEDICIÓN DEL DOCUMENTO NACIONAL DE IDENTIDAD Y SUS CERTIFICADOS DE FIRMA ELECTRÓNICA, entry into force 23.12.2005, online available: http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/reales-decretos/real-decreto-1553-2005-de-23-de-diciembre.

214. Reglement rijbewijzen, valid from 14.06.2019. Online available: https://wetten.overheid.nl/BWBR0008074/2019-06-14.

215. Regolamento per l'esecuzione delle leggi di pubblica sicurezza, entry into force 11/07/1940. Online available: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1940-05-06;635.

216. Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069653], 19/12/2018. Online available: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069653.

217. REGULATION (EC) No 444/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Online available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF.

218. REGULATION (EC) No 767/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). Online available: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32008R0767.

219. REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast). Online available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:EN:PDF.

220. REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794.

221. Regulation No. 234 Regulations Regarding Biometric Data Processing System, adopted 06.05.2014, entry into force 09.05.2014, online version available at https://likumi.lv/ta/en/en/id/266013-regulations-regarding-biometric-data-processing-system.

222. Release of information from DVLA's registers. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804462/inf266-release-of-information-from-dvlas-registers.pdf.

223. Resolución de la Secretaría de Estado de Hacienda, por la que se dictan instrucciones para el establecimiento de cauces estables de colaboración entre la Dirección General del Catastro y la

Agencia Estatal de Administración Tributaria en materia de intercambio de información y acceso directo a las respectivas bases de datos, entry into force 22/12/2003, online available: https://www.boe.es/eli/es/res/2003/12/22/(3).

224. Review of implementation of the United Nations Convention against Corruption, Executive summary: Malta. Available at: https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/13-15October2014/V1406823e.pdf.

225. Road Traffic Act 1988, online available: http://www.legislation.gov.uk/ukpga/1988/52/section/97?view=extent.

226. Road Traffic Regulations no 326 of 2014. Online available: http://www.irishstatutebook.ie/eli/2014/si/326/made/en/pdf.

227. Rozporządzenie Ministra Infrastruktury i Budownictwa w Sprawie wydawania dokumentów stwierdzających uprawnienia do kierowania pojazdami, entry into force 25.02.2016, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160000231.

228. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji zmieniające rozporządzenie w sprawie przetwarzania informacji przez Policję, entry into force 05.04.2019, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000180.

229. Rozporządzenie Rady Ministrów w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską), entry into force 24.12.2009, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20092201720.

230. SCOTTISH BIOMETRICS COMMISSIONER BILL EXPLANATORY NOTES. Online available: https://www.parliament.scot/S5_Bills/Scottish%20Biometrics%20Commissioners%20Bill/SPBill48ENS052019.pdf.

231. Social Welfare and Pensions Act no 8 of 2007. Online available: http://www.irishstatutebook.ie/eli/2007/act/8/enacted/en/pdf.

232. Standard format and technical description of an identity card and a list and the period of validity of digital data entered on an identity card, passed 02.11.2018 no 27, online available: https://www.riigiteataja.ee/akt/109112018005.

233. Statutes for maintaining of database of aliens staying or having stayed in Estonia illegally, entry into force 01.10.2010, online available: https://www.riigiteataja.ee/akt/128102016010.

234. Statutes of the border control database, entry into force 12.01.2008, online available: https://www.riigiteataja.ee/akt/112032019040.

235. Statutes of the database of border crossing queue, entry into force 15.08.2010, online available: https://www.riigiteataja.ee/akt/118092018010.

236. Statutes of the database of persons who have acquired or lost Estonian citizenship has been restored, passed 18.12.2015 nr 75, online available: https://www.riigiteataja.ee/akt/129122015001.

237. Statutes of the database of prisoners, detained persons, persons in custody and probationers, passed 01.03.2018 no 19, online available: https://www.riigiteataja.ee/akt/109032018003.

238. Statutes of the identity documents database, entry into force 01.01.2016, online available: https://www.riigiteataja.ee/akt/102022018003.

239. Statutes of the police database, entry into force 01.01.2010, online available: https://www.riigiteataja.ee/akt/112032019039.

240. Statutes of the State Register of Schengen Information System, entry into force 01.01.2010, online available: https://www.riigiteataja.ee/akt/112032019038.

241. Strafgesetzbuch, entry into force 13.11.1998, online available: https://www.gesetze-im-internet.de/stgb/BJNR001270871.html.

242. Strafprozessordnung [StPO] [Code of Criminal Procedure], Apr. 7, 1987, BGBl. I at 1074, 1319, as amended, §§ 100a-100j, http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf, *archived at* http://perma.cc/ZA7K-47GY, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf.

243. Strafprozeßordnung 1975, online available: https://tinyurl.com/y2v2h6du.

244. Strafprozessordnung, entry into force 7.04.1987, online available: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html.

245. Strafvollzugsgesetz, entry into force 26/03/1969, online available: https://tinyurl.com/y2dvjsy7.

246. Straßenverkehrsgesetz, entry into force 5.03.2003, online available: https://www.gesetze-im-internet.de/stvg/BJNR004370909.html.

247. Surveillance Camera Code of Practice, June 2013. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

248. ZÁKON 231/2019, entry into force 01/01/2020. Online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/231/20200101.

249. Zákon č. 169/1999 Sb., o výkonu trestu odnětí svobody, entry into force 01/01/2000, online available: https://www.zakonyprolidi.cz/cs/1999-169.

250. Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky, entry into force 01/01/2000, online available: https://www.zakonyprolidi.cz/cs/1999-326.

251. Zákon č. 328/1999 Sb., o občanských průkazech, entry into force 01/07/2000, online available: https://www.zakonyprolidi.cz/cs/1999-328.

252. Zákon č. 329/1999 Sb., o cestovních dokladech, entry into force 01/07/2000, online available: https://www.zakonyprolidi.cz/cs/1999-329/zneni-20180701.

253. Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích, entry into force 01/01/2001, online available: https://www.zakonyprolidi.cz/cs/2000-361?text=.

254. Zákon č. 500/2004 Sb., správní řád, entry into force 01/01/2006, online available: https://www.zakonyprolidi.cz/cs/2004-500.

255. Zákon národnej rady Slovenskej Republiky o policajnom zbore, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/171/.

256. Zákon o cestnej premávke, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2009/8/.

257. Zakon o državljanima država članica Europskog gospodarskog prostora i članovima njihovih obitelji, effective from 18.07.2019, online available: https://www.zakon.hr/z/2109/Zakon-o-dr%C5%BEavljanima-dr%C5%BEava-%C4%8Dlanica-Europskog-gospodarskog-prostora-i-%C4%8Dlanovima-njihovih-obitelji.

258. Zakon o izvršavanju kazne zatvora, effective from 2019, online available: https://www.zakon.hr/z/179/Zakon-o-izvr%C5%A1avanju-kazne-zatvora.

259. Zakon o izvrševanju kazenskih sankcij. Online available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlid=2006110&stevilka=4665.

260. Zakon o kazenskem postopku, entry into force 01.01.1995. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362.

261. Zakon o kaznenom postupku, effective from 27.07.2017, online available: https://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku.

262. ZAKON O NALOGAH IN POOBLASTILIH POLICIJE, entry into force 05.03.2013. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314.

263. Zakon o obradi biometrijskih podataka, effective from 04/01/2020. Online available: https://www.zakon.hr/z/2431/Zakon-o-obradi-biometrijskih-podataka.

264. Zákon o občianskych preukazoch, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/224/.

265. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/.

266. Zakon o osebni izkaznici, entry into force 28.05.2011. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5758.

267. Zakon o osobnoj iskaznici, effective from 06.06.2015, online available: https://www.zakon.hr/z/447/Zakon-o-osobnoj-iskaznici.

268. Zakon o policijskim poslovima i ovlastima, effective from 01.07.2009, online available: https://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html.

269. Zakon o potnih listinah, entry into force. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1598.

270. Zakon o putnim ispravama hrvatskih državljana, effective from 01.08.2015, online available: https://www.zakon.hr/z/448/Zakon-o-putnim-ispravama-hrvatskih-r%C5%BEavljana.

271. Zákon o správnom konaní (správny poriadok), online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1967/71/.

272. Zakon o strancima, effective from 26.05.2018, online available: https://www.zakon.hr/z/142/Zakon-o-strancima.

273. Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, effective from 04.08.2018, online available: https://www.zakon.hr/z/1061/Zakon-o-za%C5%A1titi-fizi%C4%8Dkih-osoba-u-vezi-s-obradom-i-razmjenom-osobnih-podataka-.

274. Zakon o tujcih, entry into force 28.07.2011. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5761.

275. Zakon o varstvu osebnih podatkov, entry into force 01.01.2005. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906.

276. Zakon o voznikih, entry into force 12.01.2017. Online available: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7164.

277. Zakon o výkone detencie, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/231/20200101.

278. Zákon o výkone detencie, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/221/.

279. Zákon o výkone trestu odňatia slobody a o zmene a doplnení niektorých zákonov, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/475/20190701.html.

280. Zákon o výkone väzby, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/221/.

281. ЗАКОН ЗА БЪЛГАРСКИТЕ ЛИЧНИ ДОКУМЕНТИ, entry into force 01/04/1999, online available: https://www.lex.bg/bg/laws/ldoc/2134424576.

282. ЗАКОН ЗА ИЗПЪЛНЕНИЕ НА НАКАЗАНИЯТА И ЗАДЪРЖАНЕТО ПОД СТРАЖА, entry into force 01.06.2009, online available: https://www.lex.bg/laws/ldoc/2135627067.

283. ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ 2014, online available: https://www.lex.bg/laws/ldoc/2136243824.

284. ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА, last modified 07.05.2019. Online available: https://lex.bg/laws/ldoc/2134163459.

285. Telekommunikationsgesetz [TKG] [Telecommunications Act], June 22, 2004, BGBl. I at 1190, as amended, §§ 110–115, http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf.

286. The Biometric Data Processing System Law of the Republic of Latvia, entry into force 24.06.2009, last amendments entry into force 19.07.2017, online version available at https://likumi.lv/ta/en/en/id/193111-biometric-data-processing-system-law.

287. The Criminal Procedure Law of the Republic of Latvia, entry into force 01.10.2005, last amendments entry into force 25.10.2018, online version available at https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law.

288. The Immigration (Biometric Registration) Regulations 2008. Online available: http://www.legislation.gov.uk/uksi/2008/3048/regulation/15/made.

289. The Law on the Procedures for Holding the Detained Persons of the Republic of Latvia, entry into force 21.10.2005, last amendments entry into force 06.03.2019, online version available at https://likumi.lv/ta/en/en/id/119371-law-on-the-procedures-for-holding-the-detained-persons.

290. The Personal Data Processing Law of the Republic of Latvia, entry into force 05.07.2018, last amendments entry into force 31.05.2019, online version available at https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law.

291. The Personal Identification Documents Law of the Republic of Latvia, entry into force 13.06.2012, last amendments entry into force 09.08.2017, online version available at https://likumi.lv/ta/en/en/id/243484-personal-identification-documents-law.

292. The Population Census Law of 2002 (141 (I) / 2002) http://www.cylaw.org/nomoi/enop/non-ind/2002_1_141/full.html.

293. Traffic Act, entry into force 01.07.2011. online available: https://www.riigiteataja.ee/en/eli/525032019002/consolide.

294. Trestný poriadok, online available: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/.

295. UK Borders Act 2007. Online available: http://www.legislation.gov.uk/ukpga/2007/30/crossheading/biometric-registration.

296. Universitätsgesetz, entry into force 01/10/2002, online available: https://tinyurl.com/kmrre8x.

297. Ustawa - Prawo o ruchu drogowym, entry into force 01.01.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970980602.

298. Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, entry into force 29.06.2002, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020740676.

299. Ustawa o Centralnym Biurze Antykorupcyjny, entry into force 24.07.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040708.

300. Ustawa o Centralnym Biurze Antykorupcyjnym, entry into force 24.07.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040708.

301. Ustawa o Dokumentach paszportowych, entry into force 28.08.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061431027.

302. Ustawa o Dokumentach paszportowych, entry into force 28.08.2006, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061431027.

303. Ustawa o Dowodach osobistych, entry into force 01.03.2015, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131.

304. Ustawa o Dowodach osobistych, entry into force 01.03.2015, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131.

305. Ustawa o Policji, entry into force 10.05.1990, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900300179.

306. Ustawa o samorządzie gminnym, entry into force 27.05.1990, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900160095.

307. Ustawa o samorządzie gminnym, entry into force 27.05.1990, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900160095.

308. Ustawa o samorządzie powiatowym, entry into force 01.01.1999, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910578.

309. Ustawa o samorządzie powiatowym, entry into force 01.01.1999, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910578.

310. Ustawa o samorządzie województwa, entry into force 01.01.1999, available online: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19980910576.

311. Ustawa o służbie wojskowej żołnierzy zawodowych, entry into force 01.07.2004, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20031791750.

312. Ustawa o strażach gminnych, entry into force 01.01.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971230779.

313. Ustawa o strażach gminnych, entry into force 01.01.1998, online available: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971230779.

314. Utlänningsdatalag 2016:27, entry into force 12.02.2016. Online available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/utlanningsdatalag-201627_sfs-2016-27.

315. Verordnung zur Durchführung des Passgesetzes, entry into force 19.10.2007, online available: http://www.gesetze-im-internet.de/passv_2007/BJNR238610007.html.

316. Verordnung über die Zulassung von Personen zum Straßenverkehr, Fahrerlaubnis-Verordnung, entry into force 13.12.2010, online available: https://www.gesetze-im-internet.de/fev_2010/BJNR198000010.html.

317. Verwaltungsstrafgesetz 1991, online available: https://tinyurl.com/ycnqaobt.

318. VILNIAUS MIESTO SAVIVALDYBĖS TERITORIJOJE ĮRENGTŲ VAIZDO STEBĖJIMO KAMERŲ IR JŲ FIKSUOTŲ DUOMENŲ NAUDOJIMO TVARKOS APRAŠAS. Online available: https://vilnius.lt/vaktai/GetFile.aspx?DocId=d797487c-e6f6-4229-abf3-1caf01c7938c.

319. Vreemdelingenwet, valid from 27.02.2019. Online available: https://wetten.overheid.nl/BWBR0011823/2019-02-27.

320. Wet houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters 2018, online available: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018112505&table_name=wet.

321. Wet identiteitsvaststelling verdachten, veroordeelden en getuigen, valid from 01.10.2010. Online availble: https://wetten.overheid.nl/BWBR0026180/2010-10-01.

322. Wet op het politieambt 1992, online available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1992080552&table_name=wet.

323. Wetboek van Strafvordering 1808, online available: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1808111730&table_name=wet.

324. Wetboek van Strafvordering, valid from 01.08.2019. Online available: https://wetten.overheid.nl/BWBR0001903/2019-08-01.

List of Court Cases

1. Case No: CO/4085/2018 between HE QUEEN (on application of EDWARD BRIDGES) and THE CHIEF CONSTABLE OF SOUTH WALES POLICE and SECRETARY OF STATE FOR THE HOME DEPARTMENT and INFORMATION COMMISSIONER and SURVEILLANCE CAMERA COMMISSIONER.

2. Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* (2014) ECLI:EU:C:2014:238.

3. Joined cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others (2016) ECLI: EU:C:2016:970.

4. Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* (2014) ECLI:EU:C:2014:238.

5. Joined cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others (2016) ECLI: EU:C:2016:970.

6. Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union (2017) ECLI:EU:C:2017:592

Miscellanea

1. About TELEFI project. Online available: https://www.telefi-project.eu/telefi-project/about-telefi-project.

2. Digital Government Factsheet 2019 – Cyprus, available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Cyprus_2019_0.pdf.

3. eDelivery in Cyprus, available at: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-cy-ia-0054.

4. EDPB. Online available: https://edpb.europa.eu/legal-framework_en.

5. Frontex, National Authorities, available at: https://frontex.europa.eu/partners/national-authorities/c.

6. Jesuit Centre for Faith and Justice, Charmaine Cristiano Grech, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Malta, available at: https://fra.europa.eu/sites/default/files/fra_uploads/malta-study-data-surveillance-mt.pdf.

7. Judicial systems in Member States – Cyprus, available at https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-cy-en.do?member=1.

8. Organization of justice – judicial systems, Malta. Available at: https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-mt-en.do?member=1.

9. Overview of German system: https://www.loc.gov/law/help/intelligence-activities/germany.php#Legislative.

10. Rights of defendants in criminal proceedings - Cyprus, available at https://e-justice.europa.eu/content_rights_of_defendants_in_criminal_proceedings_-169-CY-maximizeMS-en.do?clang=en&idSubpage=2&member=1.