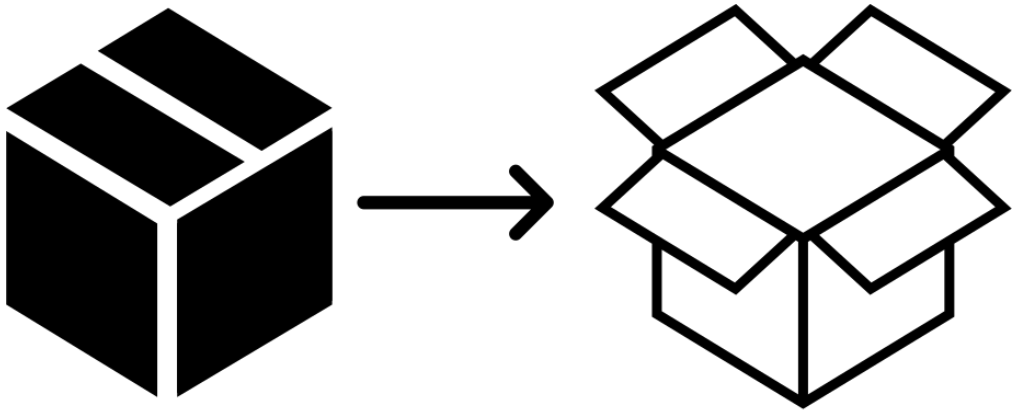
chist-era



XAIface

Measuring and Improving Explainability for AI-based Face Recognition

Legal Guidelines for AI-based Face Recognition

Deliverable number: D3.3

Version: 1.0

EURECOM Sophia Antipolis · JOANNEUM RESEARCH DIGITAL · universität wien · it · EPFL

Acronym of the project: XAIface
Title of the project: Measuring and Improving Explainability for AI-based Face Recognition.
Grant: CHIST-ERA-19-XAI-011
Web site of the project: https://xaiface.eurecom.fr/

Short abstract

Within this deliverable, legal guidelines for the application of AI-based face recognition are defined. Privacy and Data Protection (GDPR, Directive 2016/680/EU) will be addressed in particular to yield guidelines for a privacy-by-design approach specifically for AI-based face recognition. In addition, requirements of the AI Act will be addressed as well.

Table of contents

Definitions

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.[1]

Controller is a person, who alone or jointly with others decides on the means and purposes of the data processing and can be seen as the main addressee of the GDPR.

Data subjects are natural persons, whose data will be processed.

Data Protection Directive 1995 was repealed through the GDPR and was in force until the entry of the GDPR on 25th of May in 2018.

General Data Protection Regulation (GDPR): The General Data Protection Regulation is a European legal act, which lays down European-wide harmonized provisions regarding the processing of personal data and is directly applicable in all EU-member states.[2]

Personal data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[3]

Processing means any operation or set of operations which is performed on personal data or on 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.[4]

Processor is a person who processes personal data on behalf of the controller.

[1] Art. 4(1)(14) GDPR.
[2] Regulation 2016/679/EU 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[3] Art. 4(1)(1) GDPR.
[4] Art. 4(1)(2) GDPR.

1. Introduction

The ubiquity of facial recognition technology (FRT) among law enforcement authorities as well as the administration, private companies and consumers becomes more apparent by the day. The technologies are used for the purposes of identification and authentication in various use cases, from criminal law to access management of buildings. With the prevalence of the use of these systems, it is necessary to address the caveats of those use cases from a legal standpoint. These legal guidelines aim to provide general guidance on the use of such technologies with regard to the current and near future legal framework, with special regard to transparency, interpretability and explainability.

1.1. Methodology

Drawing on the principles of legal methodology, a three-step process is applied:
First, potentially legally relevant factors will be determined (legal scoping). Second, these factors will be set in context with the current legal framework, which consists of the applicable law (including EU Regulations and Directives) and case law of the ECJ (and that of other supranational courts; e.g. the ECtHR).
In order to make these guidelines applicable also to future applications, these guidelines also include (in addition to the currently applicable law) developments on the EU-level for the near future (including currently discussed Legal Initiatives with regard to software and AI; *inter alia* the Proposal for the AI Act).
Third, the relevant legal provisions are legally interpreted (interpretation of the wording and grammar, historical interpretation and teleological interpretation) to determine the extent of their application on the relevant factors in FRT (“subsumption”).

This requires the presentation of the relevant legal framework and the identification of legal issues for an in-depth legal analysis. The focus will lie on finding the relevant and applicable rules and determining how and to what extend these apply to the defined use cases of Facial Recognition Technology based on Artificial Intelligence. This is – in part – an iterative process, since the legal questions become more and more specific the more specific both view on the technological level but also the more concrete its applications become.

Where appropriate the results of the other project partners will also be incorporated into the legal assessment. Hence, the document will be continuously adapted to the results of the other WP and can be seen as a “working document”, evolving with the project progress.

The conclusions of legal assessment should – in general – always be read in light of the principle of proportionality, considering fundamental rights implications, and should ultimately provide a solid legal basis for FRT based on AI.

1.2. Objective

The goal of the version of this deliverable is to accurately map the legal framework associated with the use of FRT.

The second version will address specific use cases of FRT and their associated risks.

In addition to the legal framework, ethical and socio-political aspects will be discussed in a separate deliverable to create a holistic synopsis of the problems in the context of AI-based face recognition and its use.

In terms of content, this deliverable will deal in particular with legal issues in the area of data protection law but will also include recent European developments in the area of AI law, such as:

- General Data Protection issues in the context with FRT
- Privacy by Design requirements
- New framework within the AI Act (Proposal)

2. Legal Guidelines for AI-based Face Recognition

The application of facial recognition technology (hereinafter “FRT”) has become increasingly popular in recent years due to improvements on its performance and advanced developments in the field of computer vision. Experts predicted that the global facial recognition market will more than double in the next few years – from 3.8 billion USD in 2020 to 8.5 billion USD in 2025.[5] Even nowadays FRT is used by most people on a daily basis for instance to get access to their devices (unlocking smartphones) et cetera.

Most countries (over 80 percent) use FRT for governmental purposes and nearly 70 percent of police forces globally have access to some kind of FRT already.[6] Facial recognition is also increasingly being used by private entities; particularly biometric access control became popular over the last years since CCTV and access to appropriate analysis and evaluation software has been provided to private actors.

Once a nationwide FRT-infrastructure is installed, the possibilities of its usage will become unpredictable. Although FRT also holds beneficial uses such as assuring security (both public and private), it cannot be denied that biometric systems have the potential to endanger fundamental privacy and data protection rights. Therefore, the indiscriminate use of biometric systems must be circumvented by establishing an adequate legal framework for handling FRT and avoid extensive harm such as discriminatory measures against minorities. Also, the usage of biometric identification systems in public accessible spaces should be limited to the necessary extent in order to protect fundamental European values. Therefore, the application of FRT should only be used according to the principle of proportionality. Especially since FRT attracts much attention from the public eye due the general connotation with detrimental surveillance, privacy, and fundamental rights repercussions for the citizens a profound regulation seems inescapable.[7]

Hence, it is hardly surprising that biometric recognition processes – and especially the handling of biometric data – are subject of the European-wide political discourse and several European legal acts have already dealt with FRT-issues[8]. Nonetheless, a multiplicity of legal

[5] *Bischoff* Paul, Facial recognition technology (FRT): 100 countries analyzed, https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ (accessed on 03.08.2022); Comparitech also provided a map, where the global usage of FRT is shown.

[6] *Bischoff* Paul, Facial recognition technology (FRT): 100 countries analyzed, https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ (accessed on 03.08.2022).

[7] *New York Times*, The Secretive Company That Might End Privacy as We Know Ithttps://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (27.06.2022).

[8] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88; Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018; Directive (EU)

questions still remains unanswered and biometric systems have not been effectively regulated by the legal order yet. Thus, a profound regulation is necessary so that legal certainty is ensured.

Probably the best-known regulatory basis is the General Data Protection Regulation (GDPR), which has attracted worldwide attention due to its comprehensive regulatory content and exterritorial scope.

The GDPR applies "*to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filling system or are intended to form part of a filling system*".[9] As confirmed by previous case law, the concept of personal data is subject to an extremely broad understanding and also generally includes data processing in the context of FRT.

The systematics of the GDPR also require a legal basis for data processing; this is explicitly stated in the basic principles of data processing defined in Art 5 of the GDPR and also in the exhaustive list of legal bases in Art 6 of the GDPR. In addition to "general" personal data, the GDPR also recognizes "special categories of personal data", which are subject to a stricter standard for processing due to the increased need for protection.

In addition to the General Provisions (Chapter I) and the Principles (Chapter II), the GDPR standardizes individual rights for data subjects in Chapter III. Chapter IV regulates the responsibilities of controllers and processors and their relationship. Chapter V lays down provisions regarding the transfer of personal data to third countries or international organizations. Chapter VI and VII includes provisions regarding supervisory authorities and their mutual cooperation. Chapter VIII to XI contains provisions on remedies, liability and penalties, provisions relating to specific processing situations as well as the final provisions.

Data protection law is certainly a connecting point for regulating FRT but has already shown in recent years that it is not sufficient for AI-based processing of personal data.

Further legislative endeavours besides data protection law on a European level are already visible. The recently published proposal of the European Commission for the regulation on artificial intelligence ("Artificial Intelligence-Act"; hereinafter "AI Act (Proposal)") tries to tackle some of these issues in context with FRT and lays down certain requirements for the use of biometric systems to complete the existing data protection legislation and fill the current legal gaps.[10]

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 (Law Enforcement Directive) OJ L 119, 4.5.2016.

[9] Art 2(1) GDPR.

[10] Proposal of the European Parliament and the Council laying down harmonized rules on artificial intelligence (AI-Act) and amending certain Union legislative acts, COM(2021) 206 final.

The AI Act (Proposal) in general follows a risk-based approach based on the "pyramid of criticality", which differs between "unacceptable risk", "high-risk", "limited risk" and "minimal risk" AI-Systems.[11]

The application of remote identification systems in publicly accessible spaces for law enforcement purposes is classified as "unacceptable risk AI-systems" and thus shall be prohibited under the upcoming AI Act.[12] It should be noted that the usage of such biometric systems is not banned comprehensively since the legislative proposal provides several – relatively broad – exceptions. A total ban of certain FRTs is still being discussed, but is not part of the proposal in its current form.[13] At the beginning of the negotiations but was then dropped quite quickly since the stakeholders involved did not want to give up the benefits and economical innovation potential of FRT.

The legislative proposal also contains a catalogue of requirements for so-called "High-Risk-AI-Systems", which in the future must be operated in accordance with the new legislation.[14] Biometric identification systems will therefore either fall under "prohibited practices" or "High-Risk-AI-Systems", depending on their design and function.[15]

The scientific discourse about FRT is controversial, also with regard to the regulatory approach. – Opinions range from a total ban to soft regulation. Irrespective of this disparity of opinions, it is obvious that for the choice of regulatory instrument the nature of the technology must be considered.[16] When it comes to FRT different interests collide and must always be balanced against each other. This balancing of interests must be reflected in the regulatory framework. Different risks may arise with the processing of biometric data, depending on the design and the range of applications of the biometric system.

FRT may be used for different purposes: identification, verification and categorisation of a natural person. The human face and its intrinsically linked characteristics are the basis for the functioning of FRT. For the identification or verification of a person their facial characteristics must be retrieved, for example from photographs or video footage and then compared 1:n or 1:1, depending on the used function.[17] This process is inherent to the technology and naturally depends on the processing of "biometric" data. Different risk may arise for the data subjects, depending on the implemented technical and organizational design.

[11] *Kop* Mauritz, EU Artificial Intelligence Act: The European Approach to AI, Transatlantic Antitrust and IPR Developments (2021).
[12] Art. 5(1)(d) AI Act (Proposal).
[13] *EDPB/EDPS*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).

[14] Chapter II of the AI Act (Proposal).
[15] Art. 5(1)(d) as well as Art. 6 (2) AI Act (Proposal).
[16] See also COM, Proposal for the Regulation (EU) of the European Parliament and of the Council laying down harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM 2021/0106, 206 final, 2021/0106 (COD) p. 9
[17] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 7.

2.1. Fundamental Rights - Art. 7 and 8 of the Charta

FRT (especially real-time face recognition) are predominantly perceived by society as detrimental interferences in their rights and freedoms. It is undisputed that **FRT** – either directly or indirectly – **interfere with fundamental rights,** especially when they are used in the area of law enforcement and criminal justice.

In the European Union, fundamental rights are guaranteed by the **European Charter of Fundamental Rights** (hereinafter "Charter"). The Charter applies to all institutions, bodies, offices and agencies of the Union and to the Member States when they are implementing Union law.[18] Within the member states of the Council of Europe, the human rights of the **European Convention on Human Rights** ("ECHR") are applicable.[19] In addition the Council of Europe has addressed the issue of personal data within the **Convention 108**.[20]

For the European Union, both fundamental rights frameworks are relevant, not only because all EU Member States are also Members of the Council of Europe, but also because the Charter of Fundamental Rights is to be interpreted in conformity with the ECHR.[21] Thus, Art. 52 (2) of the Charter provides the following:

"*In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*"[22]

The use of facial recognition must be in accordance with fundamental rights.

Art. 8 ECHR ("Right to respect for private and family life") states:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

Art. 7 of the Charter ("**Respect for private and family life**") states:

"*Everyone has the right to respect for his or her private and family life, home and communications*."[23]

[18] Art. 51 of the Charter.
[19] The European Union has not yet acceded to the ECHR, but all EU member states have already ratified it; see also ECJ, Opinion of the Court (Full Court) of 18 December 2014, Opinion pursuant to Article 218(11) TFEU, Avis 2/13 - Adhésion de l'Union à la CEDH.
[20] European Council, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; see the amended version: European Council, Amending Protocol CETS No. 223 to Convention 108 (CM/Inf(2018)15-final- Convention 108+).
[21] See, for example ECJ 14 February 2019, C-345/17, *Buivids*.
[22] Art. 52(2) of the Charter.
[23] Art. 7 of the Charter.

Art. 8 of the Charter specifies a right to "**Protection of personal data**":

"1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority*."[24]

The Consultative Committee of Convention 108 has issued specific Guidelines on Facial Recognition,[25] addressing Legislators and decision-makers, developers, manufacturers and service providers as well as users of FRT.
For certain use cases, the Committee demands strict limitation by law. These include the use of live facial recognition in "uncontrolled environments" - a notion similar to publicly accessible spaces. Especially for categorisation systems, appropriate safeguards must be provided to avoid risks of discrimination.[26] Notably, the Committee also concludes that the use of biometric data processing by FRT for identification purposes should be limited to law enforcement.[27]
The European Data Protection Board (hereinafter "EDPB") has raised the issue of fundamental rights compliance in the context of FRT as well. In its Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement[28] the EDPB came to following conclusions:

The use of FRT includes the processing of personal data and mostly biometric data. Biometric data is known as special categories of personal data under the GDPR. From this data or in accumulation with other data points, conclusions could be drawn about race, ethnicity, religion, health status, etc. In addition, statements can also be made about "*habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*."[29] All this information belongs to the private life and is therefore protected under Art. 7 and, where applicable, Art. 8 of the Charter.

In addition to the fundamental rights just mentioned, **other fundamental rights may be affected** by the use of FRT.

[24] Art. 8 of the Charter.
[25] The Consultative Committee of The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition,T-PD(2020)03rev4, 28 January 2021.
[26] The Consultative Committee of The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition,T-PD(2020)03rev4, 28 January 2021, 5.
[27] Ibid., 6.
[28] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.
[29] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 12.

In a liberal society, everyone should have the right to move freely and anonymously in public without fear of discrimination, persecution, or other adverse effects. FRT could therefore also be an obstacle to the exercise of other fundamental rights, "*such as their right to freedom of thought, conscience and religion, expression of peaceful assembly and freedom of association under Articles 1, 10, 11 and 12 of the Charter*."[30] FRT also brings the risk of **treating people as mere objects**, which can never be in line with Art. 1 of the Charter "*respect and protection for human dignity*".[31]

The EDPB also states clearly that every processing of biometric data constitutes a serious interference with fundamental rights itself, independent of the outcome of the matching-process. Even in case of a "no hit" and the deletion of the biometric template, an interference has occurred.[32]

The interference with the fundamental rights may result either **from a legal act itself or from an act of an authority or private entity entrusted by law with the exercise of public power and public authority**. Regardless of this, it is always an interference with fundamental rights that requires justification.[33,34]
As stated in Art. 52(1) of the Charter "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be **provided for by law** and **respect the essence** of those rights and freedoms. Subject to the **principle of proportionality**, limitations may be made only if they are **necessary** and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*."

Thus, fundamental rights may be interfered with as long as the interference meets the requirements of the charter. A legal basis is therefore required for any interference, which must be sufficiently clearly formulated and also makes the interference foreseeable.

The **essence** of the fundamental right **can never be interfered with**. This "essence" refers to "*the very core of that right*"[35] and **must be respected under any circumstances**.[36] However, it is not always easy to determine, if this sensitive area of fundamental rights is affected or not. One boundary in any case is the human dignity which is, according to Art. 1 of the Charter an inviolable right.[37]

---

[30] *Ibid.*
[31] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 13.
[32] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 12.
[33] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 13.
[34] See also: The Consultative Committee of The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition,T-PD(2020)03rev4, 28 January 2021, 6.
[35] See ECJ, 22 December 2010, C-279/09, pt. 60.
[36] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 13; The guidelines also provide a list of indications of a possible infringement of the core on page 13.
[37] See Art. 1 of the Charter: "*Human dignity is inviolable. It must be respected and protected*."

In addition to a legal basis and consideration of the core of the fundamental right, the Charter also requires that the interference is proportionate and necessary. So, every interference must be subjected to a proportionality and necessity test.

Effective protection of fundamental rights depends not only on the scope of protection of the individual fundamental rights, but also on the possibilities for interferences. The principle of proportionality is an abstract mean to soften this tension between individual and collective interests. Necessity means that the interference must be suitable to achieve the objective pursued. If more lenient means are available and if these more lenient means can fulfil approximately the same purpose, a biometric surveillance measure cannot be considered necessary.

In conclusion, it can therefore be stated that the processing of biometric data always represents an interference with (several) fundamental rights (privacy, data protection, et cetera). For an interference with fundamental rights to be **only legally permissible it has to be specifically determined by law and suitable guarantees exist**.

Furthermore, any interference with fundamental rights must be justified and subjected to a test of proportionality and necessity. Only then can an interference be lawful.

However, it should also be taken into account when using FRT, that there exists an extremely sensitive area "the essence of the fundamental right" in which cannot be legitimately interfered. The essence represents the outermost limit for an interference with fundamental rights and must be respected under any circumstances.

3.1. General Data Protection Regulation (GDPR)

3.1.1. Introduction

With the rapid technological developments and the global increase of data processing activities, the need for a solid data protection regulation has become more important than ever. From a regulatory point of view, the text of the GDPR was designed in such a way that it would be applicable both to current and also future technological developments.[38] An adaptable framework should ensure legal certainty both for the data subjects, whose data will be processed, and for the companies and other actors, who are involved in the processing.

Due to the globally interconnected Internet economy and digitalization in general, data protection law must also be guaranteed beyond the borders of the European Union, which is why extraterritorial effects of the regulatory mechanisms are unavoidable.[39] Data protection cannot end at national borders.

Although data protection law is a relatively new area in law, as data protection was not relevant before the technological revolution. At that time, the protection of information was sufficiently covered by the fundamental right of secrecy of correspondence and secrecy of telecommunications, which still apply today, but do not guarantee an adequate protection in today's information and network society. It was not until the 1970s,[40] that the first efforts were made to create data protection law as we know it today, and it was not until the 1990s,[41] that the first legal acts were enacted within the European Union.

The former Data Protection Directive 95/46/EG already provided comprehensive protection of personal data, but had the major disadvantage that, due to it being a EU-"Directive" (instead of a directly applicable EU-Regulation) it was implemented differently from Member State to Member State.
Since May 25, 2018 the GDPR is applicable. Due to its regulatory nature (European Regulation), it entered into force directly in all Member States of the European Union without the need for transposition.

[38] Data Protection law and its regulatory mechanism are designed technology neutral.
[39] See Art. 2 GDPR.
[40] First Data Protection Law in Hessen, Germany; 1981 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) was the first binding international legal instrument in the field of data protection (available at: https://www.coe.int/en/web/data-protection/convention108-and-protocol#:~:text=The%20Convention%20for%20the%20Protection,in%20the%20data%20protection%20field, accessed: 30. August 2022).
[41] 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 L 281/31.

However, some national differences still continue to exist due to the so-called “opening clauses”.[42] . These opening clauses enable the Member States to specify certain provisions of the GDPR at the national level. This is why both national and supranational law may apply.[43] The GDPR guarantees a uniform high level of data protection in all the member states.[44]

European Data protection law is characterized by its dual purpose, its aim is, on the one hand, harmonized regulation with regard to personal data processing and, on the other hand, the guarantee of free movement of data within the European Single Market.[45] Data protection is first and foremost legal protection.[46]

The material scope of application of the GDPR is the processing of personal data.[47] Personal data can be divided into "general" and "special" personal data. With the introduction of the GDPR, biometric data were also included in the catalogue of special categories of personal data under Art. 9 GDPR.

Due to the increasing proliferation of biometric systems and their inherent processing of biometric data, it is obvious that solid regulatory approaches are inevitable. FRT encompasses the processing of biometric data and simultaneously endangers a person`s rights and freedoms (several fundamental rights may be affected), since a multiplicity of legal issues are not addressed properly by the data protection regime.[48] The current provisions of data protection law are not a sufficient regulatory tool for FRT (or AI in general), as current developments at the European level also confirm.

The following list should provide an overview of relevant data protection issues and first analysis:

1. Fundamental rights

While FRT can be used in a controlled 1:1 situation, it can also be used in a 1:n situation. If used, for example, for mass surveillance and discrimination, this would pose a high risk of intrusion into individuals’ private life (general surveillance of the crowd in publicly accessible places, etcetera). FRT could be used “*to generate a general conception of constant*

[42] See *Rücker* in Rücker/Kugler, New European General Data Protection Regulation (2018) 2.
[43] Recital 8 GDPR: “*Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law*.”
[44] Recital 6 GDPR.
[45] Art. 1(1) to (3) GDPR.
[46] *Lachmayer* in Knyrim, DatKomm Art. 1 DSGVO (Stand 1.12.2018, rdb.at) pt 27.
[47] Specifically Art. 2 GDPR.
[48] “*The use of facial recognition technologies is intrinsically linked to processing of significant amounts of personal data, including special categories of data. The face and, more generally, biometric data are permanently and irrevocably linked to a person’s identity. Therefore, the use of facial recognition has direct or indirect impact on a number of fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights that may go beyond privacy and data protection, such as human dignity, freedom of movement, freedom of assembly, and others. This is particularly relevant in the area of law enforcement and criminal justice*.“: *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26.

surveillance", which would have detrimental influence on the behaviour of the monitored public.[49] This would not be acceptable in a liberal society, since the free development of the personality and free choice of movement in a public accessible space would no longer be sufficiently guaranteed .

The right to data protection is not an absolute fundamental right.[50] Nevertheless, any interference in data protection law is only permissible to the extent that it is proportional.

2. Transparency of use

One of the main issues with FRT is the potential use without the knowledge of the data subjects.. The lack of transparency jeopardizes the exercise of the data subject's rights, which is stipulated as a key principle in data protection law and should foster the enforceability of the GDPR in general. Transparency issues will be further analysed in Section 3.1.3 as well as 3.3.6 in this document.
This is especially the case if face recognition is used remotely and for post-analysis. In a "data-generating" and "data-sharing" age the amount of footage provided for possible FRT-usage (mostly by the data subjects themselves) increases daily. Additional information can be found and linked to a natural person via their social media profiles.[51] Even though these methods are afflicted with errors, companies already demonstrated its monetary potential as well as its potential use for law enforcement purposes.[52]

3. Legal Basis

Art. 6 (1) GDPR lists six potential legal grounds for lawful processing. Theoretically, any of these legal grounds may be invoked to justify the use of FRT. One must keep in mind that in addition to a legal basis in Art. 6 GDPR, for the processing of **special categories** of personal data at least one of the exceptions in Art. 9 (2) GDPR must also apply.

With regard to Art. 6 (1) (a) GDPR, it should be mentioned that although consent is generally a valid legal ground for processing, the consent must be given explicitly due to Art. 9 (1) (a) GDPR. Since consent must also be obtained given before processing,[53], basing the processing on this legal ground is simply impractical. In many use cases, the controller cannot predict whose data will be processed (publicly accessible spaces) and can therefore not request consent beforehand. Furthermore, processing based on consent may not be valid in cases where there is a power imbalance.[54] Similarly, the use of consent as legal ground is

[49] *EDPB*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 4.
[50] Recital 4 GDPR.
[51] It is not necessary to link it to a legal recorded identity.
[52] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/ (accessed on 30. August 2022).
[53] Arg.: Art. 9(1)(a) GDPR – "has given"; "In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed." - *Art. 29 Working Party*, Guidelines on consent under Regulation 2016/679 WP 259 rev.01, 17.
[54] For example in case the controller is a public authority; for details see: *Art. 29 Working Party*, Guidelines on consent under Regulation 2016/679 WP 259 rev.01, 6.

discouraged by the Consultative Committee to Convention 108.[55] If public authorities or employers use FRTs, two main legal bases are Art. 6(1)(c) or (e) GDPR. Both of these legal bases require a formal norm either laid down by Union law or in Member State law.[56] In case the processing is based on public interest, the interest must be substantial and therefore meet a higher threshold than usual.[57]

For the area of law enforcement, the GDPR usually does not apply. However, similar requirements may be derived from the Law Enforcement Directive.[58]

4. Extent of data processing

The application of biometric identification systems does inherently process biometric characteristics of n: person. The scope of the intervention depends on the amount of identities and biometric references stored in the database. The comprehensive biometric comparison may collide with the principle of data minimization, which states that "*personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".[59]

5. Performance of FRT

The GDPR also does not provide any legal requirements how accurate an AI system must be, nor what quality the training data must demonstrate in order to counteract discrimination and similar issues in particular.

3.1.2. Personal Data and Biometric Data

This chapter analyses the handling of biometric data within the data protection law, especially the GDPR.

The material scope of the GDPR is stated in Art. 2 of the Regulation. According to Art 2(1) GDPR, it applies to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*"

It is clear from the definition, that the application of the GDPR (and of the obligations therein) is dependent primarily from the qualification of "data" as "personal" data. Personal data is defined in Art 4(1) GDPR as

"*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by*

[55] The Consultative Committee of The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition,T-PD(2020)03rev4, 28 January 2021, 6.
[56] See Art. 6(3) GDPR.
[57] See Art. 9(2) lit g GDPR.
[58] See below Section 3.2.
[59] Art. 5(1)(c) GDPR.

reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

While on the surface, Art 4(1) GDPR states that data can be qualified as "personal data" not only if the data subject is "identified" but also if it is potentially "identifiable", the provision has also another very important consequence for the legal interpretation. Art 4(1) GPDR implies that "data" (in the sense of the GDPR) primarily means "information", which is different from the technical understanding of "data". It is not the processed "data" (in a technical sense) that is either personal or non-personal, but rather the "information" that can be deducted from the processed data. This means that we cannot categorise certain types of data as being either "personal" data or not, e.g. a telephone number, an IP-address or even an image of a person, but rather must take into account the context.

This interpretation is supported by the wording of Rec 26 GDPR, which further elaborates on "identifiability" of a person under data protection law:

"*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*"

According to Rec. 26 GDPR, the determining factor is not whether the controller can identify a natural person just on the basis of the processed data, but rather the potential of the controller to combine the data with other information the controller possesses or even the means of a third party ("another person") to identify a person from that data with "means reasonably likely to be used". Therefore the processed "data" (again in a "technical" sense) is not the primary focus of the scope of the GDPR, but rather the potential information the controller (or other persons/entities) can deduct from that data (even in combination with other available information). If this can lead (reasonably likely) to the identification of a natural person, then this person is "identifiable" and the data are therefore qualified as "personal data".

While the European Court of Justice (ECJ) has elaborated this differentiated approach in the landmark case "*Breyer*",[60] it should also be highlighted – with regard to FRT –, that the recent case law of the ECJ indicates that images of a person are generally to be considered "personal data".[61] This might be the case even independent of the means reasonably likely to be used by the controller (or another person) to identify the data subject (the depicted person in the image). For FRT, this means that the use of face images should generally be considered personal data in the sense of Art. 2 and 4 GDPR.

[60] ECJ 19 October 2016, C-582/14, *Breyer*.
[61] ECJ 14 February 2019, C-345/17, *Buivids*

The GDPR emphasizes the importance of biometric information, by including biometric data in the definition of "special categories of personal data" (Art. 9(1) GDPR) for the first time.[62] The repealed *Data Protection Directive 95/46/EG* did not mention biometric data explicitly. Hence, a legal definition of the notion "biometric data" in the context of processing personal data exists since the entry into force on the 25th of May in 2018. With the classification as special categories of personal data, data subjects enjoy a higher level of protection (e.g. stricter requirements for the Lawfulness of the processing, et cetera) with regard to the processing of "biometric data".[63]

Art. 4(1)(14) GDPR defines biometric data as follows:

***"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".*[64]

Like any other AI, FRT requires data to train and to develop. The development of FRT, however, requires the processing of personal data, i.e. physical, physiological or behavioural characteristics of the data subjects, which are linked to a person's identity. Physical characteristics may be the human face, iris, or fingerprints. Behavioural characteristics would be keystrokes, voice or gait as well as the signature of a person.[65]

Due to the inherent nature of these characteristics, facial data is not only personal, but also personalized. Biometric features thus have several advantages over traditional authentication components such as knowledge and possession, but their misuse can also lead to detrimental repercussions for the concerned person. On the one hand, biometric information can neither be forgotten nor (easily) exchanged. This might be welcome from a security perspective, but if the information gets compromised (e.g. identity theft) it will be compromised forever since it cannot be replaced or exchanged like a conventional mean of knowledge (e.g. PIN, password,..) or possession (cards,.). The risk of a life-long compromise poses a major problem.

However, for completeness it must also be pointed out that within the category of biometric features, different strengths and weaknesses of the features exist and not every feature is equally suitable for identifying the person properly. Behavioural characteristics in particular stand out as active characteristics since they can be influenced by the "feature carrier" himself or changed over time by nature or artificial processes. The human face in fact is a quite suitable biometric feature, as it is on the one hand easy to capture (and without the knowledge

[62] The repealed Data Protection Directive 95/46/EC neither defines "biometric data" nor classifies biometric data as special categories of personal data; Recital 51 GDPR.
[63] Art. 9(1) GDPR.
[64] Art. 4(1)(14) GDPR.
[65] See Gola in *Gola*, DSGVO - Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar[2] (2018) Art. 4 pt. 96.

of the feature carrier) and on the other hand relatively consistent. Although the human face is subject to a natural process of change due to ageing, the technological means have advanced to a point where FRT can adapt to the ageing process and the person can most likely be identified. Nonetheless, plastic surgeries or similar proceedings may have an influence on the performance of FRT.[66]

Even though the definition of the notion laid down in the GDPR is quite similar to the technical understanding of biometric data, differences exist. Within the GDPR biometric data will only be generated if the processing aims to allow or confirm the identification of the natural person. By implication any biometric classification, which does not allow or confirm the identification of the data, will not be seen as the processing of biometric data under the GDPR.

According to the definition of biometric data, personal data can only be qualified as "biometric data" if it is processed using a specific technology. Naturally, face recognition carried out by a human does not fall under the processing of biometric data in the sense of the GDPR. Even though facial images are explicitly cited in the definition, facial images are biometric data only if the processing purpose aims for **uniquely identifying a natural person**.[67] This also requires that the "means" of the processing[68] must be suitable in a certain processing situation to allow or confirm an identification.

3.1.3. Transparency and Explainability

3.1.3.1. General Remarks

First, the terms "transparency" and "explainability" must be defined. Depending on the chosen definition, requirements towards transparency and explainability may vary.[69] The general model relied upon in this analysis was developed by *Waltl & Vogl and* defines transparency and interpretability as subcategories of explainability.[70] The definition of "explainability" may differ depending on the field. The High-Level Expert Group on Artificial Intelligence of the European Union, for example, holds the view that explainability would only be a subcategory of transparency.[71]
For the GDPR Wachter et alia conducted one of the first main analysis of a "right to explanation". The broader concept of "explainability" (Waltl & Vogl) fits the elaborated

[66] See the results of WP 2, where certain influencing factors are analysed in detail.
[67] *EDPB*, Guidelines 3/2019 on processing of personal data through video devices, p. 15; *Hödl* in *Knyrim* (Hrsg.), DatKomm Art 4 DSGVO (Stand 1.12.2018, rdb.at) 148 ff; *Schulz* in *Gola/Heckmann* (Hrsg.), Bundesdatenschutzgesetz §46 Bundesdatenschutzgesetz Rn 64; *Albers/Veit* in *Wolff/Brink (*Hrsg.), BeckOK Datenschutzrecht, Art 9 Rn 44.
[68] Compare to Art. 4(7) GDPR according to which a processing activity is essentially determined by its purpose and means.
[69] For preliminary work, see Deliverable 4.1.
[70] *Waltl/Vogl*, Explainable artificial intelligence – the new frontier in legal informatics, in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/Legal Tech – Proceedings of the 21st International Legal Informatics Symposium IRIS 2018 (2018) 118.
[71] *High-Level Expert Group on AI,* Ethics Guidelines for Trustworthy AI (2019) 18.

approach of *Wachter et alia,*[72] and is therefore better suited as a baseline for the further discussion in this section.

Even after deciding on a model, transparency may still refer to various different obligations. According to a study prepared for the Members of the European Parliament, "algorithmic transparency" may relate to various aspects such as code, logic, model, goals and decision variables.[73] Furthermore, transparency models can be either "global" or "local", referring to either the system as a whole or a specific input respectively.[74] The authors further distinguish depending on the potential areas of transparency, such as data, algorithms, goals, outcomes, compliance, influence and usage. Lastly, one must differentiate based on potential addressees of transparency. Information may be provided to authorities, third-party analysts, researchers or be generally available to everyone.[75]

The term transparency therefore refers to the provision of information to a select group of addressees about the facial recognition systems, potentially including the code, the logic, the model, input, output and further details.Transparency can be seen as a subcategory of explainability.
Further determination depends on the specific context and will be elaborated below.

The term "*explainability*" has no agreed-upon legal definition. However, various authors have attempted to define related terms, especially within the context of the debate on the "*right to explanation*". The debate concerned the specific rights awarded to data subjects within the framework of the GDPR. The right to explanation could potentially be based on provisions including – but not limited to – Art. 13, 14, 15 and 22 GDPR. These provisions of the GDPR relate to "automated decision-making", which are defined in the GDPR itself. Hence, the provisions require an automated **decision** and not only a specific technology or technical system. Whether or not a decision by a facial recognition system needs to be "explained" therefore depends on the specific use case.

According to *Wachter et alia* explanations can be categorized into **two categories**. The first category concerns **system functionality**, which would include information about the logic of the system, significance, envisaged consequences, decision trees, pre-defined models, criteria and classification structure.[76] The second category consists of **explanations of specific decisions**, which includes the rationale and reasons, weighting of features and profile groups.

The *Wachter et alia* further distinguish between different potential explanations depending on the time they are given: An ***ex ante* explanation** would naturally be limited to the first set of factors. An ***ex post* explanation** could also include specific decisions. Whether explanations

[72] *Wachter/Mittelstadt/Floridi*, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law (2017) Vol. 7/2, 76.
[73] *EPRS,* study: A governance framework for algorithmic accountability and transparency (2019) 4.
[74] *EPRS,* study: A governance framework for algorithmic accountability and transparency (2019) 5.
[75] *EPRS,* study: A governance framework for algorithmic accountability and transparency (2019) 6.
[76] *Wachter/Mittelstadt/Floridi*, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law (2017) Vol. 7/2, 76.

according to the GDPR have to be provided and if they have to contain both sets was subject to debate[77] and is currently content of preliminary ruling procedures by the ECJ.[78]

Further legal obligations to explanation may be derived from the Art. 35 GDPR on the data protection impact assessment and will be highlighted in the section below. Additionally, the GDPR does not apply in every potential use case of facial recognition based on machine learning. In the area of criminal law, transparency obligations or a right to explanation may be derived from national law, which is in turn based on the EU Directive 2015/680. Specifities of Directive 2015/680 are discussed in a separate section below.

It should be noted that not every decision based on facial recognition technology falls within the scope of Art. 22 GDPR. The right to explanation in its current form only applies insofar as a decision was rendered without significant human involvement and if the decision has legal consequences or similar effects. The meaning of these two limitations remains subject to academic debate.[79]

3.1.3.2. Transparency according to the GDPR

Even though transparency is not explicitly defined in the GDPR, Recital 39 GDPR establishes that transparency is a principle of the regulation. According to Recital 39 GDPR, "*it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed*".[80]

Art. 5(1)(a) GDPR elevates **transparency** to one of the **key principles**, alongside lawfulness and fairness. According to one of the central authorities, the Article 29 Working Group, the aim of transparency in the GDPR is to enable data subjects to exercise their rights. Furthermore, transparency is a part of accountability.[81] The material scope of transparency according to Art. 2 GDPR is limited to wholly or partly automated processing of personal data and is an obligation of the controller towards data subjects as well as a right of data subjects.

The modalities of transparency are defined in Art. 12 GDPR, whereas specific contents of transparency obligations can be found in Art. 13 and 14 GDPR. Art. 15 GDPR defines the right of the data subject to obtain information as a counterpart to the obligations of the previous articles. Art. 12 GDPR demands that the provision of information must be concise, transparent, intelligible and easily accessible. The language must be clear and plain and the provision of information must be free of charge.

---

[77] *Kim/Routledge*, Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach (2020)(available at: http://dx.doi.org/10.2139/ssrn.3716519, accessed: 30. August 2022).
[78] LVwG Wien 11.02.2022, VGW 101042791/2020.
[79] For details see *Wendehorst*, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021) 52.
[80] Rec. 39 GDPR.
[81] *Art. 29 Working Party*, Guidelines on transparency under Regulation 2016/679 – WP 260 rev.01 (2018) 5.

"**Intelligible**" can be defined as understandable for the average reader.[82] "Readability testing" is recommended by the Art. 29 Working Party. The obligation should not be overlooked, since the standards are high. Information can be made easily accessible through pop-ups or highlighted privacy notices. It should be noted, that in line with the system of the GDPR it is generally not the obligation of the data subject to actively seek out information, but rather for a controller to provide it.[83] Even though some exceptions allow for oral provision of information, written or electronic form is usually required. The recommended approach is a **layered privacy notice**.[84]

Privacy notices may also include forms of visualisation. Visualisation may only be used as an addition to natural language.[85] Certain information according to Art. 13 & 14 GDPR should be provided in combination with standardised icons. In general, however, other visualisation tools such as data protection seals and marks may be used.[86]

The contents of the obligation to transparency are defined in Art. 13 & 14 GDPR. While Art. 13 GDPR addresses the scenario, in which personal data was obtained from the data subject, Art. 14 GDPR covers those cases, where data was not obtained (directly) from the data subject. While the core information the controller is required to provide is the same, these provisions still differ slightly. Seeing as in the scope of Art. 14 GDRP, personal data wasn't obtained from the data subject, additional information has to be provided – including on the source of the data. An overview is provided by the Article 29 Working Group in the guidelines on transparency.[87]

3.1.3.3. Obligations under Art. 22 GDPR

Art. 22 GDPR ("*Automated individual decision-making, including profiling*") contains additional transparency obligations that are, however, only applicable in the very restricted scope of Art. 22 GDPR.

Although Art. 22 GDPR mentions "*profiling*" in its title, this is partly misleading. This is the case because on the one hand, "profiling" is not a necessary requirement for the application of Art. 22 GDPR (arg.: "*including*") and on the other hand, only profiling as part of an automated decision-making, which also produces legal effect or similarly significantly affects the data subject are covered under Art. 22 GDPR. The Art. 29 Working Party in its Guidelines on Automated individual decision-making under the GDPR[88] has described this as following:

"*There are potentially three ways in which profiling may be used:*

[82] *Art. 29 Working Party*, Guidelines on transparency under Regulation 2016/679 – WP 260 rev.01 (2018) 7.
[83] Ibid.
[84] For further instructions on layered privacy notices see *Art. 29 Working Party*, Guidelines on transparency under Regulation 2016/679 – WP 260 rev.01 (2018).
[85] *Franck* in *Gola*, DS-GVO[2] (2018) Art. 12(47).
[86] For further information, see preliminary work in D 4.1.
[87] *Art. 29 Working Party*, Guidelines on transparency under Regulation 2016/679 – WP 260 rev.01 (2018).
[88] *Art. 29 Working Party*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 – WP 251 rev.01 (2018).

(i) general profiling;
(ii) decision-making based on profiling; and
(iii) solely automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject (Article 22[1]).

The difference between (ii) and (iii) is best demonstrated by the following two examples where an individual applies for a loan online:

- *a human decides whether to agree the loan based on a profile produced by purely automated means(ii);*
- *an algorithm decides whether the loan is agreed and the decision is automatically delivered to the individual, without any prior and meaningful assessment by a human (iii).”*[89]

However, the Art. 29 Working Party also comes to the conclusion that ”*the controller cannot avoid the Article 22 provisions by fabricating human involvement […]*” and that “*to qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture*”.[90]

In addition, Art. 22 GDPR only applies to cases, where the automated decision has either a “*legal effect*” (as in the establishment or the cancellation of a contract) or “*similarly significantly affects him or her*”, e.g. their financial circumstances, their access to health services or has an effect on other “significant” circumstances.[91]

If the use of FRT based on AI has such a legal or “similar” effect, this requires the controller to specifically inform the data subject of

"*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*" according to Art. 13 (2)(f) and 14(2)(g) GDPR.

3.1.4. Privacy-by-Design

Art. 25 GDPR requires the controller to take certain steps on “Data protection by design and by default". To design a system so that it implements "*data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of* [the GDPR] *and protect the rights of data subjects*" according to Art. 25 GDPR, requires

[89] Ibid., 8.
[90] *Art. 29 Working Party*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 – WP 251 rev.01 (2018) 21.
[91] *Art. 29 Working Party*, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 – WP 251 rev.01 (2018) 22.

an understanding of the architecture of such a system. Like with common AI systems, the system functions can be structured in data collection, data organization, analysis and infusion.[92]

3.1.4.1. General remarks

The underlying idea of "Privacy-by-Design" is that compliance with the GDPR shall be part of the technical (or organisational) system – non-compliance with the GDPR should be made impossible by technical means.[93] Technology should be a mean to enforce data protection law.[94]

Addressee of the duties laid down in Art. 25 GDPR is the controller, even if the controller did not design or implement the system used for processing himself.[95] The controller would be the entity that operates the system, even if it uses AI frameworks provided by private companies. First, the controller must implement appropriate technical and organizational measures, which are designed to implement data-protection principles, in an effective manner.

This requires measures, which effectively implement the principles of processing personal data. These principles are according to Art. 5 GDPR:

- lawfulness, fairness and transparency,
- purpose limitation,
- data minimization,
- accuracy of data,
- storage limitation,
- integrity and confidentiality,
- accountability.

These measures do have to prevent every data protection infringement; they just have to be designed in a way to effectively serve the purpose.[96] Measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk.[97]

Not all measures have to be of a technical nature since the regulation explicitly mentions organizational measures. Therefore, training of personnel can also be a valid measure.[98]

---

[92] *See* https://www.ibm.com/cloud/architecture/architectures/aiAnalyticsArchitecture/reference-architecture/ (accessed on 2. October 2022).
[93] *Bergauer* in Jahnel, Kommentar zur Datenschutz-Grundverordnung (2021) Art. 25 pt 1.
[94] *Hötzendorfer/Kastelitz/Tschohl* in Knyrim (Hrsg.), Der DatKomm, 7. Lfg. Art. 25 pt 4.
[95] *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pt 4.
[96] See *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pt 22.
[97] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 7.
[98] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 6.

Second, the controller must integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

These safeguards should address the following requirements of the GDPR:

- provision of sufficient guarantees to implement appropriate technical and organizational measures by processors, engagement of other processors only with prior authorization, closing of a processor's agreement (Art. 28 GDPR)
- record of processing activities (Art. 30 GDPR)
- cooperation with the supervisory authority (Art. 31 GDPR)
- implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR)
- compliance with notification and communication duties in case of data breaches (Art. 33, 34 GDPR)
- data protection impact assessment (Art. 35 GDPR)
- designation of a data protection officer, who can act effectively (Art. 37 et seqq. GDPR)
- transfer of personal data only under the conditions of the GDPR (Art. 44 et seqq. GDPR)

In addition, these measures should improve the accessibility of the following rights of the data subjects:

- transparent information and communication (Art. 12-14 GDPR)
- right of access (Art. 15 GDPR)
- right to rectification (Art. 16 GDPR)
- right to erasure (Art. 17 GDPR)
- right to restriction of processing (Art. 18 GDPR)
- right to data portability (Art. 20 GDPR)
- right to object (Art. 21 GDPR)
- right not to be subject to a decision based solely on automated processing (Art. 22 GDPR)

These measures and safeguards must be defined at the time of the determination of the means for processing. Therefore, already the specifications of the system to be implemented must cover technological and organizational measures which address all of these principles.[99] Data protection and security should be provided in a verifiable manner via quality management throughout the whole life cycle of the software.[100] The controller must re-evaluate his processing operations through regular reviews and assessments of the effectiveness of the chosen measures and safeguards.[101]

Assessing which measures are to be implemented the controller has to take into account the state of the art (meaning the current progress in technology that is available in the market has

[99] See *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pt 17.
[100] *Tretzmüller*, Privacy by design in der Softwareentwicklung, ZIIR 2020, 145.
[101] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 11.

to be taken account of),[102] the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (risk-based assessment on the principle of proportionality).[103]

When performing the risk analysis for compliance with Article 25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments.[104] The EDPB Guidelines on Data Protection Impact Assessment can also be used in an assessment according to Art. 25 GDPR.[105]

The principle of privacy by design you also find in the eIDAS regulation, in connection with an interoperability framework for national electronic identification schemes.[106]

ENISA names eight privacy design strategies:[107]

- **minimize**: restrict the amount of personal data to the minimal amount possible; design patterns include “select before you collect” and “anonymization and use pseudonyms”
- **hide**: hide personal data, and their interrelationships, from plain view; design patterns include encryption, mix networks to hide traffic patterns, anonymization and pseudonymization,
- **separate**: process personal data in a distributed fashion, in separate compartments whenever possible,
- **aggregate**: process personal data at the highest level of aggregation and with the least possible detail in which it is (still) useful; design patterns include aggregation over time, k-anonymity, differential privacy,
- **inform**: whenever data subjects use a system, they should be informed about which information is processed, for what purpose, and by which means,
- **control**: provide data subjects agency over the processing of their personal data; design patterns includes user centric identity management and end-to-end encryption,
- **enforce**: put a privacy policy compatible with legal requirements in place and enforce it; design patterns include access control, sticky policies and privacy rights management,
- **demonstrate**: be able to demonstrate compliance[108] with the privacy policy and any applicable legal requirements; design patterns include privacy management systems and the use of logging and auditing.

[102] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 8.
[103] *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pt 12.
[104] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 9.
[105] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 10.
[106] Art. 12 section 3 lit c Reg(EU) 910/2014 of 23.7.2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[107] ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014, 18 seqq. (available at: enisa.europe.eu, accessed on 28. June 2022).
[108] See also *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 7.

The controller should have **documentation of the implemented technical and organizational measures**. To do so, the controller may determine appropriate key performance indicators to demonstrate the effectiveness. Alternatively, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.[109] Another form of safeguards are measures that make processing contrary to the intended purpose visible (e.g. logging features).[110]

A certification of the system or certain processing operations can help to prove compliance with Art. 25 GDPR.[111]

The following examples can be given in respect to an FRT system based on AI:

3.1.4.2. Lawfulness, fairness and transparency

The characteristics of AI including opacity ("black box-effect"), complexity, unpredictability and partially autonomous behaviour, may make it hard to verify compliance with this principle.[112] However, transparency could be improved by keeping accurate records regarding the data set used to train and test the AI systems, including a description of the main characteristics and how the data set was selected. In certain justified cases, keeping the data sets themselves and keeping a documentation on the programming and training methodologies, processes and techniques used to build, test and validate the AI systems.[113]

Lawfulness of the processing must be secured. The information duties in respect to the data subjects according to Art. 12-14 GDPR must be fulfilled. In addition, an access interface could be implemented,[114] via which data subjects could find out if their face data is part of a data set (and could demand that their face data is to be deleted).

3.1.4.3. Purpose and storage limitation

Usually purpose limitation, by its very nature, will not be possible in a true big data aggregation, since the very idea of a data aggregation is to generate yet unknown later analysis and network

[109] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 7.
[110] *Hötzendorfer/Kastelitz/Tschohl* in Knyrim (Hrsg.), Der DatKomm, 7. Lfg. Art. 25 pt 24.
[111] See *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (20.10.2020) 29.
[112] European Commission, Whitepaper "On Artificial Intelligence - A European approach to excellence and trust" COM(2020) 65 final, 12 (available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, accessed 27. June 2022).
[113] European Commission, Whitepaper "On Artificial Intelligence - A European approach to excellence and trust" COM(2020) 65 final, 19 (available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, accessed on 27. June 2022).
[114] *Bergauer* in Jahnel, DSGVO Art. 25 pt 11.

effects big data applications.[115] However, here face data could be deleted automatically if it is not longer needed,[116] e.g. if the AI has been sufficiently trained on it.

3.1.4.4. Data minimization

The frame for measures to ensure data minimization is quite narrow, since one can not determine beforehand, which part of face data will improve the AI trained on it.

3.1.4.5. Accuracy of data

Determining the accuracy of the face data is an inherent purpose of the system and therefore it would not be necessary to address this aspect in particular.

3.1.4.6. Integrity and confidentiality

AI systems must be technically robust and accurate to be trustworthy. Measures can include internal requirements ensuring:

- that the AI systems are robust and accurate, or at least correctly reflect their level of accuracy, during all life cycle phases,
- that outcomes are reproducible,
- that AI systems can adequately deal with errors or inconsistencies during all life cycle phases,
- that AI systems are resilient against both overt attacks and more subtle attempts to manipulate data or algorithms themselves, and that mitigating measures are taken in such cases.[117]

In respect to system architecture, the strategy to “separate” mentioned above requires that processing of personal data in the main functions (data collection, data organization, analyzation and infusion) should be conducted in separate compartments of the system, so the compromising of the security of one compartment doesn’t lead to the compromising of the whole system.

3.1.4.7. Accountability

Specifications, documentation, and the results of the regular reviews of the system must show that the necessary technical and organizational measures and safeguards have been implemented. In case of an incident the log files of the system should be so detailed and tamper-resistant, that the extent of a data breach can be determined.

---

[115] *Wilmer*, Rechtliche Rahmenbedingungen für KI Systeme. Immanente Herausforderungen und mögliche Lösungen durch Control by Design, TATup 2021 30/3, 56-62, with reference to *Holthausen*, Big data, people analytics, KI und Gestaltung von Betriebsvereinbarungen. Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, RdA 74(1) 19–32.

[116] *Bergauer* in Jahnel, DSGVO m Art. 25 pt 11.

[117] European Commission, Whitepaper “On Artificial Intelligence - A European approach to excellence and trust” COM(2020) 65 final, 20 f (available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, accessed on 27.6.2022).

3.1.4.8. Privacy by Default (Section 2)

In addition, the controller has to implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Here the principle of proportionality doesn't apply; the controller has to ensure that only the necessary date is processed.[118] The controller is obliged to implement measures to ensure an overshooting processing is not possible.[119]

Second, the provision also has the goal to ensure that data subjects themselves using the system are confronted with default settings which do not lead to the disclosure of personal data but require active action by the data subject if he wants to make his data accessible to a great number of recipients.[120]

3.1.5. Data Protection Impact Assessment ("DPIA") – Art. 35 GDPR

This section determines the prerequisites in respect to Art. 35 GDPR for a system for AI-based face recognition.

A data protection impact assessment (in the following "**DPIA**") is a process designed to explain the data processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs help controllers not only to **comply** with requirements of the GDPR, but also to **demonstrate that appropriate measures have been taken** to ensure compliance with the GDPR.[121]

3.1.5.1. Determining the Necessity of a DPIA

General remarks

A DPIA must only be carried out if a type of processing is likely to result in a **high risk** to the rights and freedoms of natural persons. Art. 35(3) GDPR gives three **examples** – systematic and extensive evaluation of personal aspects, processing of special categories of personal

[118] *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pt 20, 22.
[119] *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pt 20, 23.
[120] *Bergauer* in Jahnel, Kommentar zur DSGVO Art. 25 pts 20, 24.
[121] *Article 29 Data Protection Working Party*, Guidelines 4/2019 on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, rev .01 (4.10.2017) 4.

data on a large scale and systematic monitoring of a publicly accessible area on a large scale. These examples are, however, not exhaustive.

“High risk to rights and freedoms”

According to the Article 29 Data Protection Working Party (in the following “WP29”) a **risk** is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. The **rights and freedoms** affected by the risk primarily refers to the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.[122]

First it has to be assessed, if the aggregation of face data sets, the use of AI techniques to generate artificial face images and making the aggregated data available falls into **one of the categories mentioned in Art. 35(3) GDPR**, where a DPIA is mandatory:

a) **Systematic and extensive evaluation of personal aspects** relating to natural persons which is based on automated processing, including profiling, and on which **decisions** are based that produce legal effects concerning the natural person or similarly significantly affect the natural person

b) Processing on a **large scale of special categories** of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10 DGPR

   Although there is a great uncertainty, which image data must be considered as belonging to **special categories** of data,[123] the processing at hand can nconsidered as a processing of special categories of data on a large scale. This is based on the assumption, that the image data at hand doesn’t include assets for biometric use – in that case a special category according to Art. 9(1) GDPR would apply (see Art. 4(14) GDPR: “*‘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*”).

   Apart from special categories of personal data other (“normal”)categories of personal data can also be considered as increasing the possible risk for the data subjects. These could be linked to household and private activities (e.g. confidential electronic communication) or impact the exercise of a fundamental right (e.g. location data questioning the freedom of movement) or data which violation involves serious

[122] *Article 29 Data Protection Working Party*, Guidelines 4/2019 on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, rev .01 (4.10.2017) 6.
[123] In depth discussed by *Jahnel* in Jahnel, Kommentar zur Datenschutz-Grundverordnung (2021) Art. 9 pt 23.

impacts in the data subject's daily life (e.g. financial data that can be used for payment fraud) and are therefore regarded as **sensitive data**.[124]

However, depending on its quality, it could be used for identity theft in a "video ident" procedure (identity theft is explicitly addressed as a risk under Recital 75 GDPR). Therefore, if such image data would be processed on a **large scale**, a DPIA would be necessary. What constitutes a large scale is not specified which is why the WP29 recommends considering the number of data subjects concerned, the volume of data respectively the range of different data items, the duration or permanence of the processing and its geographical extent, for this assessment.[125]

c) **Systematic monitoring** of a publicly accessible area on a large scale

The WP29 names **nine criteria**, which should be considered to determine, if a processing is likely to result in a high risk. In most cases a processing activity meeting two of these criteria would require a DPIA, however also just meeting one of these criteria can require a DPIA:[126]

1. **Evaluation and scoring**: This would include profiling and predicting and especially cover aspects like performance at work, economic situation, health, personal interests, reliability and behaviour, location or movements (similar to the case of Art 35(3)(a) GDPR).

2. **Automated decision making with legal or similar significant effect**: This means processing that aims at taking decisions on data subjects producing legal or similarly significant effects - see also section a) above.

3. **Systematic monitoring**: This covers processing used to observe, monitor or control data subjects, not only but including publicly accessible areas - see also section c) above.

4. **Sensitive data or data of a highly personal nature**

5. **Data processed on a large scale**:

[124] *Article 29 Data Protection Working Party*, Guidelines 4/2019 on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, rev .01 (4.10.2017) 9 f.
[125] *Article 29 Data Protection Working Party*, Guidelines 4/2019 on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, rev .01 (4.10.2017) 10.
[126] *Article 29 Data Protection Working Party*, Guidelines 4/2019 on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, rev .01 (4.10.2017) 9 f.

6. **Matching or combining datasets**: This includes combining data sets originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

   This will mostlikely be the case with FRT since aggregation of face data sets is one of the main purposes of the processing.

7. **Data concerning vulnerable data subjects**: This criterion addresses a power imbalance between the controller and the data subjects, which can make the data subjects unable to easily consent to, or oppose, the processing of their data, or exercise their rights. These include children, employees, mentally ill persons, asylum seekers, elderly, patients and any other cases with similar imbalances.

   Since there is a high probability that face datasets include images of vulnerable data subjects, this criterion should be kept in mind with regard to FRT..

8. **Innovative use or applying new technological or organizational solutions**: Here WP29 names the combining use of fingerprint and face recognition for improved physical access control as an example and explains, that the use of new technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms - indeed, the personal and social consequences of the deployment of a new technology may be unknown.

   This is another highly relevant criterion with regard to the application of FRT (aggregation of face data sets and the use of AI technology).

9. **Processing itself prevents data subjects from exercising a right or using a service or a contract**: This includes processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

3.1.5.2. Conclusion

At least three criteria as defined by the WP29 are highly relevant for FRT and there is a substantial probability that two additional criteria are fulfilled. It is suspected that for many use cases of FRT a DPIA is necessary.

The DPIA has to be carried out **prior to commencing** with the processing (Art. 35(1) GDPR). According to German authorities this includes not only the implementation of the measures but also the testing of their effectiveness.[127]

[127] *Trieb* in Knyrim (Hrsg.), Der DatKomm, 32. Lfg. Art. 35 pt 89.

3.1.5.3. Contents of the DPIA - Overview

According to Art. 35(7) GDPR the DPIA must contain at least:

(a) A systematic **description of the envisaged processing operations and the purposes** of the processing, including, where applicable, the legitimate interest pursued by the controller.

(b) An **assessment of the necessity and proportionality** of the processing operations in relation to the purposes. According to the literature, especially the conflict of interest between the controllers and the data subjects must be assessed in a DPIA regarding artificial intelligence.

(c) An **assessment of the risks** to the rights and freedoms of data subjects. According to Recitals 84 and 90 this includes an evaluation of origin, nature, particularity, likelihood and severity of these risks.

(d) The **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

3.2. Law Enforcement Directive (Directive [EU] 2016/680)

Directive (EU) 2016/680 (Law Enforcement Directive – in the following "LED") is part of the data protection reform package together with the GDPR. Unlike the „General" Data Protection Regulation, the LED regulates a **specific area of data protection law**:

„*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.*" (Art. 1(1) LED)

This means that the scope of application is already formulated in a very limited way, both materially and personally.

The scope of application of the LED is special in that data processing by the police and judiciary was previously (under the Lisbon Treaties) assigned to the so-called "*Third Pillar*" of the European Union, which was only regulated by international cooperation of the Member States and not by uniform legal acts by the European Union. Only with Art. 16 Treaty on the Functioning of the European Union (TFEU)[128] a special legal basis was created, which enabled this area of data processing to be subject to uniform regulation.[129]

This also explains the different choice of legal acts for the GDPR (EU Regulation; directly applicable in national law) and LED (EU Directive; must first be implemented by the Member States in national law). While only some supplementary regulations may be created in national law for the GDPR, the LED must be fully implemented in the respective national law. The statements provided here refer exclusively to the provisions of the LED and not to national implementations.

The scope of application is limited **personally** in that it only applies to the „**competent authorities**".[130] „Competent authorities" in the sense of Art. 3(7) LED are those bodies and institutions, to which the exercise of official authority or sovereign powers for these purposes has been conferred to by law – even if only on a case-by-case basis.[131] Only if **official authority** has been directly transferred, the processing is covered by the scope of application; the mere order by a competent authority to collect data for these purposes is not sufficient.[132]

Furthermore, the scope of application is **materially** limited to

[128] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 2012/326, 47-390.
[129] *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz (2018) 29-30.
[130] *Bresich et al*, DSG – Datenschutzgesetz Kommentar (2018) § 36 pt 1.
[131] *Bresich et al*, DSG – Datenschutzgesetz Kommentar (2018) pt 12.
[132] *Bresich et al*, DSG – Datenschutzgesetz Kommentar (2018) pt 15.

„*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*“ (Art. 1(1) and 2(1) LED)

According to Rec. 13 LED, a **criminal offence** within the meaning of the LED should be „*an autonomous concept of Union law as interpreted by the Court of Justice of the European Union*“. (Rec. 13 LED). However, Member States can, according to the Commission, also „*rely on the notion of criminal offence as defined in their national legal systems“.*[133] *A* distinction must be made between administrative and criminal offences (e.g. that lead to criminal procedure or typical criminal sanctions such as imprisonment).[134]

Both definitions[135] and structure of the LED are similar to those of the GDPR. According to Art. 4(1) LED fundamental principles relating to processing of personal data are defined, that are identical to that of Art. 5(1) GDPR. Art. 8 to 10 LED set out the specific conditions, under which processing of personal data in the law enforcement context[136] is to be considered lawful. Art. 8 LED can be considered a „translation“ of Art. 6 GDPR: both provisions set the basic conditions for the lawfulness of the processing of personal data. While Art. 6(1) GDPR contains six different bases for lawful processing of personal data,[137] Art. 8(1) LED has only one: the necessity for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) LED and that the processing is based on Union or Member State law. Art. 8(1) LED therefore is comparable to Art. 6(1)(e) GDPR.[138]

With Art. 10 LED, there is also a specific provision within the LED, concerning the **processing of special categories of personal data**. According to Art. 10 LED Member State law may only allow 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*“ (i.e. special categories of personal data[139])

[133] EU Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Minutes of the ninth meeting of the Commission expert group on the Regulation [EU] 2016/679 and Directive (EU) 2016/680, 4.5.2017, 1; see also *Bresich et al*, DSG – Datenschutzgesetz Kommentar (2018) pt 2.

[134] EU Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Minutes of the ninth meeting of the Commission expert group on the Regulation [EU] 2016/679 and Directive (EU) 2016/680, 4.5.2017, 1.

[135] The definitions in Art. 3 LED are, for the most part, identical to those in Art. 4 GDPR.

[136] In the sense of Art. 1(1) LED.

[137] I.e.: **consent** of the data subject or the necessity for the performance of a **contract**, for the compliance with **legal obligations**, for the protection of **vital interests**, for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller or, lastly, for the purposes of the **legitimate interests** pursued by the controller or by a third part Art. 6(1) GDPR.

[138] Art. 6(1)(e) GDPR: „*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*“.

[139] See the title of Art. 10 LED.

where this is **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.

According to the wording of Art. 10 LED, these additional requirements (authorised by Union or Member State law, vital interests, or data manifestly made public by the data subject) are equal alternatives, where the applicability of only one would seem to allow the processing of special categories of personal data.

Furthermore, the LED contains provisions on „automated individual decision-making“ (Art. 11 LED; see also Art. 22 GDPR); on general obligations of the controller (Art. 19 et seqq LED) including the obligation on data protection by design and by default (Art. 20 LED), records of processing activities (Art. 24 LED), and the data protection impact assessment (Art. 27 LED; DPIA). Art. 29 et seqq regulate data security as well as data breach notifications. Transfers to third countries must abide by the rules set out in Art. 35 et seqq.
There are, however, a few important **differences** between the **two legal acts** that are also of relevance to processing activities concerning facial recognition technology based on AI.

First, Member States are explicitly required to provide for appropriate **time limits** for the erasure of personal data or for a periodic review of the need for the storage of personal data according to Art. 5 LED. This goes beyond the general “storage limitation” principle as stated in Art. 4(1) (e) LED (or Art. 5(1) (e) GDPR), in so far as the time limit makes an assessment of the necessity of further storage of the data unnecessary (or at least sets fixed dates for the assessment as part of a periodic review).

According to Art. 6 and 7 LED, the national law should require the controller to make a clear distinction between **different categories of data subjects** as well as of personal **data based on facts** from that **based on personal assessments**.

The requirement of “*distinction between personal data and verification of quality of personal data*” under Art. 7 LED can be understood to a higher standard of documentation. It requires the competent authority to provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.[140]

There is also a specific requirement in Art. 25 LED for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. According to Art. 25 LED, the logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.[141]

[140] See especially Art. 7(1) LED.
[141] Art. 25(1) LED.

According to Art. 25(2) LED, these logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

However, while the standard of the documentation obligations can be considered higher than those in the GDPR, the transparency obligations must be considered to be of a somewhat lower standard, because of the potential limitations in national law. This is due to the nature of law enforcement procedures including criminal investigations, which could be severely hampered, if the information would have to be provided at the beginning of the processing activity to the data subject (e.g. a suspect). This means that under the LED, exemptions of these transparency obligations apply more often than under the GDPR.

While Art. 13 LED contains a transparency obligation regarding the data subject (that is comparable to Art. 14 GDPR), and a right to access in Art. 14 LED, there are also potentially wide reaching exceptions from these obligations: First, Art. 13 (3) LED lists the following grounds, under which the information to the data subject under Art. 13 (2) LED can be restricted:

a. avoid obstructing official or legal inquiries, investigations or procedures;
b. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c. protect public security;
d. protect national security;
e. protect the rights and freedoms of others.

The remaining information obligation according to Art. 13 (1) LED – there are no exemptions for these in Art. 13 LED – do not require the controller to inform the data subject directly.

According to the Art. 29 Working Parties "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", "the way and timing" for providing these informations is different in Art. 13(1) compared to 13(2) LED, because their wording is different. While Art. 13(1) LED requires the controller "to make available" information to the data subject, Art. 13(2) LED requires the controller "to give" information to the data subject in "specific cases". In addition, Rec. 42 LED points out the option of making the (basic) information according to Art. 13(1) LED about the controller and processing activities available on the **website** of the controller.[142]

More specifically: if **FRT is used by competent authorities** for law enforcement purposes as defined in Art. 1(1) LED and the national transposition act, the controller would have to "**make available" (e.g. on the website)** the fact that this technology is employed as well as the **purposes of the processing** for which the personal data are intended.[143]

Secondly, the right of access by the data subject according to Art. 14 LED can be restricted according to Art. 15 LED, insofar as that is necessary in order to

[142] Rec. 42 LED.
[143] In addition to other information requirements under Art. 13(1) LED (i.e. identity of the controller; data protection officer; the right to lodge a complaint with a supervisory authority and contact details; the existence of the right to access, rectification, restriction or erasure of personal data).

a. avoid obstructing official or legal inquiries, investigations or procedures;
b. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c. protect public security;
d. protect national security;
e. protect the rights and freedoms of others.

3.3. Proposal for the AI Act

On the 21th of April 2021, the European Commission officially proposed the first regulation on Artificial Intelligence (AI Act [Proposal]).[144] According to the Explanatory Memorandum, the regulation would have a twin objective: to promote the uptake of AI and to address the risks with those technologies. The proposal is set out to become a horizontal legal framework for trustworthy AI in the European Union. National authorities will be responsible to enforce this framework. The underlying theme of the Regulation is to protect human rights. However, systematically it is part of the product security legislation. As of now, the proposal is being discussed in the Council (of the European Union) and changes to the text are to be expected. Nevertheless, some outlines seem quite clear already and the guidelines must therefore incorporate this second central regulation for facial recognition technology based on AI (beside the GDPR).

According to Art.1 AI Act (Proposal), the Regulation aims to lay down harmonised rules for the internal market. Hence, the guidelines must address which new rules will apply and elaborate on their respective implications. Some artificial intelligence practices will be prohibited and some will have additional requirements if they are found to have a higher risk. Therefore, guidance must be provided on avoidance of prohibited practices and compliance with the additional requirements.

3.3.1. Scope of the Proposed Regulation

Like most of EU Regulations, the text encapsulates the scope in Art.2 AI Act (Proposal)l, and can be divided into two components: the territorial scope and the material scope of the provisions.

Art. 2(1) defines the territorial scope and clarifies that the regulation, much like the GDPR, is not strictly restricted to the territory of the European Union.

The regulation applies to providers of AI systems, which are put into service in the European Union, irrespective of where their establishment is situated. Even if providers and users of AI systems are solely located in a Non-EU state, the regulation may apply, if "*the output produced by the system is used in the Union*"[145]. This scope is, however, limited through the Art. 1(4)4 AI Act (Proposal): "*This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph*

[144] COM,
[145] Art. 1(1)(c) AI Act (Proposal).

1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States." Naturally, also users of AI systems located in the territory of the European Union fall in the scope. The terms "provider" and "user" are defined in Art.44 AI Act (Proposal).

Art. 2(2) AI Act (Proposal) creates an exemption for most of the provisions for systems, which are covered by other, more specific safety regulations. Those areas mainly concern vehicles such as trains, automobiles, planes and transport in general.

Art. 2(3) AI Act (Proposal) also exempts any AI system developed exclusively for military purposes.

The further material scope is tied to the word 'artificial intelligence system'. According to Art. 3(1) AI Act (Proposal), an AI system "*means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;*".

The first significant part of the definition is the word "*software"*. It clarifies that no hardware components, such as sensors, are needed for a system to be considered AI. The system must be developed with one or more of the techniques listed in Annex I AI Act (Proposal).

Those techniques and approaches include the following:

"*(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;*

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods."[146]

This list of techniques is broad, but exhaustive. According to the Explanatory Memorandum,[147] the definition should be "technology neutral" and "future proof". Still, a fixed list of techniques and approaches was created to provide legal certainty. Annex I of the AI Act (Proposal) is part of the delegated acts (to the European Commission), which means that more regular changes are possible to accommodate for rapid technological advances.[148]

[146] Annex I AI Act (Proposal)..
[147] COM, Proposal for the Regulation (EU) of the European Parliament and of the Council laying down harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM 2021/0106, 206 final, 2021/0106 (COD) p. 12.
[148] See Article 4 AI Act (Proposal). (Amendments to Annex I)

Furthermore, a system must have objectives, which were defined by a human and generate outputs. Some examples such as ‘content’, ‘predictions’ or ‘decisions’ are given. These outputs must influence the environments they interact with.

3.3.1.1. Subsumption “Artificial Intelligence System”

“AI-based” face recognition will only have to conform with the provisions of the regulation, if the system can be subsumed under the definition of ‘Artificial Intelligence System’ according to Art. 3(1) AI Act (Proposal). Definitions of Artificial Intelligence used in other disciplines do not necessarily coincide with this specific legal definition.[149]

The first criterion of the definition – software – is unproblematic and will always be fulfilled.

These guidelines focus on FRT systems based on machine learning. The definition explicitly lists a variety of machine learning approaches, be it supervised or unsupervised. The systems will also generate an output. To evaluate what these outputs are, if the system has human defined objectives and is influencing the environment they interact with, one must consider the specific use case. These points cannot be assessed independently of the specific environment a system is used in.

However, there is a high probability, that facial recognition systems will also fulfil those criteria, as demonstrated by the hypothetical scenario below:

Example 1:

An enterprise installs a security system on their premises including ‘smart’ cameras. The cameras conduct facial scans. The output of the system is the (non-)identification of a specific person. The output can already be considered a decision if no further human intervention is envisaged (‘This is person A’). This decision prevents certain persons on a blacklist from gaining access to a building by automatically locking a door or keeping said door locked. The system had an effect on the environment (locked door). The human-defined goal for the system was to provide security by identifying people and preventing some of them from entering.

This analysis must be conducted for each use case. In the opinion of the authors, influencing the environment cannot only be interpreted as having an influence on a simple software and hardware environment. The term can incorporate the human component, meaning that people may be the environment itself that is influenced. This interpretation is mainly derived from the usage of the word ‘recommendation’ in the definition, which by nature is usually directed solely towards a human counterpart.

[149] See *Norvig/Russell*, Artificial Intelligence: A Modern Approach, Global Edition[4] (2021); see also *Zanol/Buchelt/Tjoa/Kieseberg*, What is “AI”? - Exploring the Scope of the “Artificial Intelligence Act” in: Schweighofer/Saarenpää/Eder/Zanol/Schmautzer/Kummer/Hanke, Recht DIGITAL - 25 Jahre IRIS, Proceedings of the 25th International Legal Informatics Symposion IRIS 2022 (2022) 25.

3.3.1.2. "Biometric Data"

Some applications of AI receive special requirements even within the high-risk category and are therefore defined in Art. 3 AI Act (Proposal). The common denominator of these systems is the use of "biometric data".

"Biometric data" is defined as "*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*".[150]

This definition is identical with the definition of biometric data in the GDPR.[151] The choice to adopt the same definition as in the GDPR leads to the conclusion that the same interpretations should be applied to the provision in the AI Act (Proposal), including relevant jurisdiction.[152]

3.3.1.3. "Emotion Recognition System"

The first listed technology is an "emotion recognition system", which refers to "*an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data*."[153] .

3.3.1.4. "Biometric Categorisation System"

A "**biometric categorisation system**" refers to "*an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data*".[154] The system does not identify any natural person, but rather categorizes them based on chosen criteria inherent to their biometry.

3.3.1.5. "Remote Biometric Identification System"

"Remote biometric identification system" refers to "*an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified*".[155] As opposed to the biometric categorization system, the identification process of individual persons is the main purpose of the system.

Systems come in two different variations:

[150] Art. 3(33) AI Act (Proposal).
[151] Art. 4(14) GDPR.
[152] See section on biometric data.
[153] Art. 4(34) AI Act (Proposal).
[154] Art. 4(35) AI Act (Proposal).
[155] Art. 4(36) AI Act (Proposal).

a) "**Real-time remote biometric identification system**": "*a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention*."[156]

b) "**Post remote biometric identification system**": "*a remote biometric identification system other than a 'real-time' remote biometric identification system*."[157]

Both definitions are relatively self-explanatory. Where the first refers to a use case, in which the system processes either a "live feed" or similar data stream, the second case is negatively defined and refers to any usage of an identification system after the fact.

3.3.2. Prohibited Practices

Art. 5 AI Act (Proposal)contains a list of prohibited practices. While it is not unfathomable that a facial recognition system based on AI would be part of any system listed in Art. 5(1)(a) – (c)[158], the central provision is Art. 5(1)(d):

"*the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:*

(i) the targeted search for specific potential victims of crime, including missing children;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

(iii) *the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA 62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State*."

Art. 5(1)(d) AI Act (Proposal)contains a general prohibition to use real time remote biometric identification systems in public spaces. A publicly accessible space is defined as "*any physical place accessible to the public, regardless of whether certain conditions for access may apply*".[159]

Publicly accessible must be interpreted more extensively.

[156] Art. 4(37) AI Act (Proposal).
[157] Art. 4(38) AI Act (Proposal).
[158] See for example the usage of facial recognition software for social credit systems: *Everling*, Social Credit Rating (2020).
[159] Art. 3(39) AI Act (Proposal).

Example 2:

A public university provides space for leisure, learning, meetings and sports activities on their own campus. The area is partially open-air, partially indoors and surrounded by a large fence. In order to gain access, one must provide either a student or staff license or a visitor's pass. On a daily basis hundreds of students and visitors frequent the area.

Locations such as this university campus may be considered "publicly accessible", even if one might need to be a student, staff or a registered visitor to enter it.

The provision contains some exemptions, which are an expression of the proportionality principle. Certain public interests outweigh the risk of the usage. While Art. 5(1)(d)(iii) is defined very clearly, parts of the other exemptions will probably have to be clarified throughout the further process or later on by jurisdiction.[160]

Example 3:

At 06:30h local time, the Dutch police receive a credible and concrete threat and a tip from Europol, that a person is planning to shoot random passengers at Amsterdam Central Station at 08:30. Documents of the potential shooter are stored in the Europol Information System (EIS). It is currently rush hour at Amsterdam Central Station and the police does not want to cause a panic, but rather identify and apprehend the potential shooter, before any harm is caused. Alarming the potential shooter by sending multiple squads in to comb the area could result in him opening fire. Fortunately, the station is equipped with multiple video cameras. The police run a scan of the live feeds and cross reference with the biometric data stored in the Europol database. The potential perpetrator is identified by the system and apprehended. The operation ends, the system is deactivated.

Note: The usage of the system is not legitimized by the provision in the proposal of the AI-Act. The Dutch police, the judiciary organs, Europol and other involved agencies still have to comply with the respective national laws and the respective European data protection law. However, since there was a substantial (death or bodily harm) and imminent (within the next one or two hours) threat to the life or physical safety of natural persons or (depending on the motivation) a terrorist attack and the crime could be prevented, the exemption may apply. The necessity could arguably be based on the fact that no alternatives with the same outcome and lower risk to the people were available.

Example 4:

At 18:30h local time, the Austrian police receive a call from a curator at the Viennese Museum of Modern Art, that two men and a woman, who look like the suspects in a recent robbery of a Klimt painting are currently wandering around in their museum and inspecting works of art.

[160] Arg.: „*specific potential victims*".

The suspects potentially robbed and illicitly trafficked works of art all around Europe. When the police arrive, they have not been seen on the cameras for two minutes. The police use the life feeds from the exit and around the immediate area and a compatible facial recognition software to detect, localize and apprehend the suspects. The operation ends, the system is deactivated.

Note: The use of the system is not legitimized by the provision in the proposal of the AI-Act. The Austrian police and the judiciary organs still have to comply with the respective national laws and the respective European data protection law. The aim is to detect and localize the suspects of a recent robbery of a Klimt painting and trafficking of multiple works of art. A Klimt painting can be considered a "work of art" or a "cultural good" as referred to in Art. 2(2) of Council Framework Decision 2002/584/JHA 62 (European Arrest Warrant). Illicit trafficking of works of art or cultural goods is in the scope of the provision. Robbery per se is only subject to the provision, if the perpetrators were organized or armed. Additionally the crime must be "punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State" for the exemption to apply. The maximum custodial sentence for robbery as member of a criminal organization, for example, would be 15 years[161] in Austria. Hence, the exemption may apply.

As noted in the example, the exemptions may apply. The scenarios do not only need to pass the necessity test, but also pass further restrictions according to Art. 5(2) AI Act (Proposal), if the systems are used for the purposes of law enforcement.

The following elements need to be taken into account:

"*(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;*

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences."[162]

These provisions extend the necessity test, which was already mentioned before, to a proportionality test. In the cases mentioned above, the law enforcement agencies must weigh the public interest against individual rights and freedoms of all persons concerned. This does not only mean the potential suspects or perpetrators, but also any passer-by for example.

Additionally, the use of real-time biometric identification systems for law enforcement purposes in publicly accessible spaces must comply with certain safeguards. Those safeguards must be necessary and proportionate.[163]

According to the provision, the use shall be limited temporally, geographically and personally. If we take a look at the examples, those safeguards and limitations can be easily illustrated:

[161] See § 143(1) Austrian Criminal Code.
[162] Art. 5(2) AI Act (Proposal).
[163] Art. 5(2) AI Act (Proposal).

Safeguards in Example 3:

- The system is not used without prior cause. The cause is a tip from Europol and a credible and concrete threat.
- Geographical limitation: The system is only used within the station, the area of the potential crime, not in the whole city.
- Temporal limitation: The system is only used until the suspect is apprehended.
- Personal limitation: The system only scans people within the station.

Safeguards in Example 4:

- The system is not used without prior cause. The cause is a call from the curator of the Museum of Modern Art.
- Geographical limitation: The system is only used within and around the museum, the area where the suspects were spotted and likely still are.
- Temporal limitation: The system is only used until the suspects are apprehended.
- Personal limitation: The system only scans people within the immediate area and the exit.

As noted in the examples, the use of the systems is not automatically legitimized by falling in the scope of one of the exemptions. The systems must be used in accordance with national criminal procedure and (European) data protection law. As such, the usage of facial recognition systems and the respective data processing without cause for the purposes of law enforcement will usually not be in accordance with data protection law.[164]

The AI Act (Proposal)also limits the usage of facial recognitions systems further by demanding "prior authorization granted by a judicial authority or by an independent administrative authority of the Member State"[165]. An exception can be made in case of urgency. Authorization may then be requested *post factum*.

The respective judicial authority or independent administrative authority should only grant such requests if the use is necessary and proportional, including the establishment of the aforementioned safeguards.

Furthermore, the request itself must be defined by the law.[166] As a consequence, a Member State will most likely have to create new legislation detailing the requests, the objectives and modalities of the usage of such systems.

Overall, it is apparent that the aim of these provisions is not to generally prohibit the use of FRTs in publicly accessible spaces for the purposes of law enforcement. Rather, the use will be limited to certain cases.[167]

[164] See ECJ, 8.04.2013, C-293/12 and C-594/12 ('Digital Rights Ireland').
[165] Art. 5(3) AI Act (Proposal).
[166] Art. 5(4) AI Act (Proposal).
[167] *Geminn*, Die Regulierung Künstlicher Intelligenz, ZD 2021, 354 (357).

3.3.2.1. Relevant Opinions on the Provisions on Biometric Systems

The European Economic and Social Committee highlighted, that “post” and “near” biometric recognition does not fall within the scope of the provision. Likewise, systems with a purpose other than identification (e.g.: emotion recognition) will not be covered by the prohibition.[168] The prohibitions are also limited to law enforcement.

The EDPS and EDPB argue in a joint opinion, that automated biometric recognition in public spaces should be prohibited as a whole due to the high risk the use case poses for fundamental rights.[169]

3.3.3. Classification as High Risk System

A core principle of the AI Act (Proposal)is the risk-based approach. The risk-based approach was chosen to ensure effective and yet proportionate rules for AI-systems.[170] Another expression of this approach, besides the prohibition of certain practices, is the classification of specific use-cases as “high-risk”. Those systems will have to comply with additional requirements, such as human-oversight and data governance obligations.

The classification as a high-risk AI system is outlined in Art. 6 AI Act (Proposal):

“*1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:*

(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.”

[168] *European Economic and Social Committee*, Opinion AI/Regulation - Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts [COM(2021) 206 final - 2021/106 (COD)] INT/940 (2021) 5.
[169] *EDPB/EDPS*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).
[170] See Rec. 14 AI Act (Proposal).

According to Art. 6 AI Act (Proposal)the **classification as "high-risk AI system**" depends on specific use cases. In essence, there are two options on how an AI system may be classified as "high risk":

Either the system is a safety component or a product covered by Union harmonization legislation listed in **Annex II** and must undergo a third-party conformity assessment. This concerns safety components of and products like toys[171], machinery[172] or medical products[173].

According to Art. 6 AI Act (Proposal), this would also concern motor vehicles[174], which are covered by legislation listed in Section B of Annex II. However, according to the scope defined in Art. 2 AI Act (Proposal), most of these systems only have to comply with Art. 84 AI Act (Proposal). The purpose of this construct is currently being questioned in literature[175] and may likely change in the future.

If a system is not covered by the legislation mentioned in Annex II or does not have to undergo a third-party conformity assessment, it will still be classified as high-risk-system, if it represents a **use-case mentioned in Annex III**.

3.3.3.1. Opinions on the classification system

Both options for classification are criticized in position papers, since the assessment will be done by providers of AI-systems, but depends on the specific use cases of those systems. Providers, however, are **not able to anticipate** all possible use cases of their systems and

[171] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1).
[172] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24) [as repealed by the Machinery Regulation].
[173] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1.
[174] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1); 3. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1
[175] *Bomhard/Merkle,* Regulation of Artificial Intelligence, EuCML 2021, 257 (260).

are therefore not capable of providing an all-encompassing assessment.[176]. Furthermore, the classification does not take into account certain criteria such as exclusion and inexplicability.[177]

3.3.3.2. Systems according to Annex III

The central provision for classifying FRT-systems as "high-risk" will be paragraph 1 of Annex III AI Act (Proposal):

"*High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:*

1.Biometric identification and categorisation of natural persons:

(a) *AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;*"

If FRT-systems are not prohibited by Art. 5 AI Act (Proposal) or can benefit from one of the exemptions and may therefore be used – provided the usage is compliant with other legislation – they will be categorized as high-risk if they are intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons.

Even though the provision states, that AI-systems must be intended for the 'real-time' ***and*** 'post' remote biometric identification of natural persons, it should be read as "**either** 'real-time' ***or*** 'post'", as it is clearly the intention of the Proposal to categorize a system as high-risk even if it fulfils only one of those criteria. The provision may be changed in the future.

Importantly, this specific provision on categorization does not require the system to be intended to be used in the context of law enforcement. Hence, this provision may apply to use-cases in various sectors.

Example 5:

The facts are based on Example 1, where a private establishment makes use of an entrance security system, employing FRT-systems. "Building Security Ltd.", a company specializing in security systems for buildings, installed the smart cameras and accompanying software. Their system falls in the scope of Annex III(1), since it identifies natural persons through biometrics in 'real-time'. Building Security Ltd, the provider, must classify the system as "high-risk".

If the broad provision in Annex III AI Act (Proposal)(1) does not apply to the system, it may still be classified as high-risk based on other usages listed in Annex III.

[176] *EDPB/EDPS,* Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).
[177] *European Economic and Social Committee*, Opinion AI/Regulation - Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts [COM(2021) 206 final - 2021/106 (COD)] INT/940 (2021) 6.

Annex III AI Act (Proposal) contains specific provisions for use cases in a law enforcement context such as paragraph 6(c) for the detection of deep-fakes, or (d) for the evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences and others. Another possible example covered by Annex III could be monitoring in the context of labour.[178]

However, Annex III AI Act (Proposal) is likely to change during the course of the legislative process and even afterwards, since the competence to change it is essentially delegated to the European Commission.[179]

3.3.4. Requirements for High Risk Systems

AI systems, which are not prohibited by Art. 5 of the proposal and are classified as high-risk according to Art. 6 of the proposal, must adhere to additional requirements according to Article 8 of the proposal.

The obligations according to Chapter 2 AI Act (Proposal) include the following:

- Establishment of a risk management system (Art. 9)
- Data and data governance requirements (Art. 10)
- Technical documentation (Art. 11)
- Record-keeping (Art. 12)
- Transparency and provision of information to users (Art. 13)
- Human oversight (Art. 14)
- Accuracy, robustness and cybersecurity (Art. 15)

The guidelines will only further elaborate on the data and data governance requirements, as well as the transparency and human oversight requirement.

3.3.5. Data and Data Governance

Any AI-System, which is classified as “high-risk”, must comply with the obligations set out in Title III of the proposal. However, the obligations differ depending on the techniques employed. If the creation of a system involves the training of models with data, the requirements in Art. 10 (2-5) AI Act (Proposal) must be observed. For AI-systems other than those, only Art. 10(2) must be observed.[180]

These requirements concern the use of **data for training, validation and testing.** Data governance in the sense of Art. 10 means providing for appropriate data governance and management practices. These requirements will for the most part have to be satisfied before

[178] Annex III(4)(b) AI Act (Proposal).
[179] See Art. 7 AI Act (Proposal).
[180] Art. 10(6) AI Act (Proposal).

the system is in operation and aresimilar other assessments in European data protection law in that respect.[181]
According to Art. 10(2), these design choices pertain to:

- "*the relevant design choices;*
- *data collection;*
- *relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;*
- *the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;*
- *a prior assessment of the availability, quantity and suitability of the data sets that are needed;*
- *examination in view of possible biases;*
- *the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.*"

Additionally, Art. 10(3) AI Act (Proposal) postulates the requirement that all mentioned data sets "shall be relevant, representative, free of errors and complete. The interpretation of this clause is subject to academic debate. It is especially questionable what the term "free of errors" is supposed to encapsulate. Practically, and with special regard to large data sets, it should be virtually impossible to ensure complete freedom from errors.[182] The requirement of using representative data sets is furthered through the inclusion of the obligation to use appropriate statistical properties as well as paragraph 4, which requires the provider to take into account the context in which the system will be used (e.g. geographical).

Art. 10 AI Act (Proposal)naturally has a certain proximity to the corpus of EU data protection regulation. As established beforehand, any data usage that falls within the scope of the GDPR must necessarily be based on one or more of the legal grounds enlisted in Art. 6 GDPR. Further restrictions may apply mainly according to Art. 9 GDPR for special categories of personal data, which includes biometric data. Similar obligations apply with regard to other contexts such as law enforcement. Any usage of special categories of data must therefore be justified appropriately.

Art. 10(5) AI Act (Proposal)facilitates the usage of such data for the purposes of "*ensuring bias monitoring, detection and correction in regulation to high-risk AI systems*". The data may be used, but only to the extent, it is **strictly** necessary for said purpose. Appropriate safeguards must be set up, which include:

- technical limitations on the re-use
- use of state-of-the-art security and privacy preserving measures

Such measures may consist of pseudonymisation and encryption. Where possible, the data should be anonymised.[183] The provider of a high-risk AI system must draft up technical

[181] *Bomhard/Merkle,* Regulation of Artificial Intelligence, EuCML 2021, 257 (260).
[182] *Bomhard/Merkle,* Regulation of Artificial Intelligence, EuCML 2021, 257 (260).
[183] Art. 10(5) AI Act (Proposal).

documentation[184] This technical documentation includes information about data used for validation and testing as well as potentially discriminatory impacts.[185]

Art. 10(5) AI Act (Proposal)provides a new legal ground for data processing of special categories of biometric data, which includes biometric data. The provision makes use of the exception in Art. 9(2)(g) GPDR.[186] The GDPR remains applicable independently (i.e. in addition to the proposal). Therefore, any processing based on this provision must be in the public interest and substantial. This will not always be the case for any system.

Alternatively, data processing may be done within the framework of a regulatory sandbox.[187] Regulatory sandboxes may be established by one or more Member States or the European Data Protection Supervisor. At its core, the sandbox is supposed to be a controlled environment. Its purpose is to facilitate the development, testing and validation of innovative AI systems. Insofar as the development, testing or validation includes data processing, the competent data protection authorities must be involved.[188]

Art. 54 AI Act (Proposal)will provide a basis for data processing within the framework insofar as the AI system is in the public interest. The relationship of the article to the GDPR framework is currently unclear and is heavily criticized.[189] The debate focuses on the classification of the legal ground as further processing in the sense of Art. 6(4) GDPR and the possibility of reconstruction and deanonymisation of the processed data after the fact. Details will likely be left to national legislation.

3.3.6. Transparency & Explainability

While the proposal contains various provisions on transparency, interpretability and traceability, the concept of “explainability” is, similar to the GDPR, not explicitly laid down in the provisions. Recital 38 AI Act (Proposal)recognizes that explainability may be considered a necessity for certain use cases: “*[T]he exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not* ***sufficiently transparent, explainable and documented****. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress.*”

[184] Art. 11 AI Act (Proposal).
[185] Annex IV(2)(g) AI Act (Proposal).
[186] *Ebert/Spiecker*, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188 (1191).
[187] Art. 53, 54 AI Act (Proposal).
[188] Art. 53(2) AI Act (Proposal).
[189] *EDPB/EDPS,* Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021) 18; *Ebert/Spiecker*, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188 (1192).

At the current state, however, this is the only mention of a word akin to explainability in the Proposal. Even though this is surprising, it should be noted that the provisions are still subject to change and the provisions on transparency and explainability in the GDPR as well as the LED remain unaffected. However, the scope of these provisions is severely limited.[190]

Even though explainability is not a core concept of the proposal, obligations to increase transparency, interpretability and traceability can be found scattered in the obligations for providers and users. The main provisions on transparency are Articles 13 & 14 AI Act (Proposal).

Art. 13 AI Act (Proposal)contains design requirements. According to Art. 13 High-risk AI systems must be designed and developed in such a way that their operations are **sufficiently transparent to the user**. The user must be able to interpret the outputs. The aim of the provision is to enable the relevant actors to comply with other provisions set out in the AI Act (Proposal).

Any High-risk AI system must be accompanied by "instructions". The set of instructions may be delivered digitally or other format. The instructions must contain "*concise, complete, correct and clear information that is relevant, accessible and comprehensible to users*"[191]

The information according to Art. 13(3) AI Act (Proposal)includes key points about the provider as well as information about the system, such as :

- Intended purpose
- Accuracy, robustness and cybersecurity level
- Reasonably foreseeable misuse causing risks to health, safety and fundamental rights
- Performance "*as regards the persons or groups of persons on which the system is intended to be used*"
- Information about training, validation, testing data sets and input data
- Human oversight measures

It should again be noted that a user in the sense of the Proposal is usually a professional user, (a company for example), not a consumer and therefore in most use cases not equal to the data subject.

Art. 14 AI Act (Proposal)contains the requirement to design and develop High-risk AI systems in such a way that they can be effectively overseen by natural persons in production. This obligation contains the requirement to create an appropriate human-machine interface.[192]

[190] For a detailed analysis on Art. 14 of the Proposal and Art. 22 GDPR see: *Wendehorst*, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021) 52.
[191] Art. 13(2) AI Act (Proposal).
[192] Art. 14(1) AI Act (Proposal).

The aim of human oversight is to prevent and minimise risks. Human oversight measures must be identified and built in by the provider or be identified by the user.[193] The measures are not explicitly listed. Instead, a set of goals is provided in Art. 14(4) AI Act (Proposal)4.

The person overseeing the system must be able to fully understand the capacities and limitations of the high-risk AI system and be able to detect anomalies and dysfunctions.

Furthermore, this person must "remain aware" of automation bias, which is defined as "*the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons*".[194]

The person must be able to correctly interpret the outputs, "*taking into account in particular the characteristics of the system and the interpretation tools and methods available*".[195]

The provisions contain a requirement for the person overseeing the system to always be able to not use, disregard, override or reverse the output as well as to stop the system as whole.[196]

3.3.7. Art. 14 of the Proposal & Facial Recognition

Facial recognition technology will have to comply with the special paragraph on biometric systems[197] in Art. 14 AI Act (Proposal). This concerns real time as well as post remote biometric identification of natural persons. According to this provision, "*no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.*" The usefulness of the provision is already questioned due to the lack of guidance and means for compliance.[198]

3.4. Conclusion

As a first conclusion, it must be highlighted, that the legal framework for facial recognition is manifold and diverse. The pertinent rules are always tied to the specific use case, the context in which a system is used, because the legal framework is generally "technology neutral".

For public authorities and bodies, the articles of the Charter of Fundamental Rights may apply and significantly limit the usage of FRT.

The processing of biometric data represents an interference with (several) fundamental rights (privacy, data protection, etcetera). An interference with fundamental rights must be determined by law. Appropriate safeguards must be provided.

[193] Art. 14(2) AI Act (Proposal).
[194] Art. 14(4)(b) AI Act (Proposal).
[195] Art. 14(4)(c) AI Act (Proposal).
[196] Art. 14(4)(d),(e) AI Act (Proposal).
[197] Systems according to Annex III(1)(a) AI Act (Proposal).
[198] *Wendehorst*, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021) 102.

Furthermore, any interference with fundamental rights must be justified and subjected to a test of proportionality and necessity for the interference to be considered lawful.

With regard to secondary law, either the law enforcement directive or the GDPR will apply – with some exceptions for bodies of the European Union or international organizations.

These frameworks not only oblige controllers of FRT systems to justify the processing and enable the data subjects to exercise their rights, but also to comply with specific design requirements such as data privacy by design and default. FRT technology for the purpose of identification and authentication usually processes biometric data, meaning that further restrictions to the processing apply. Additionally, most controllers will have to conduct an impact assessment.

The Proposal for an “AI Act” generally classifies many applications of FRT as high-risk, depending on the specific use case. According to Art. 5 of the Proposal, some use cases of FRT will be prohibited. This concerns the usage of real-time FRT for law enforcement purposes in publicly accessible spaces. Exemptions may apply provided appropriate safeguards have been implemented.

The Proposal will force providers and users of high-risk AI systems to comply with extensive requirements, which – among others – will include the requirement to set up a risk management system, technical documentation, logging and ensure accuracy, robustness and cybersecurity.

During the design and development phase, special attention must be paid to the data used for training, validation and testing. The provider is required to eliminate biases. To that end the provider may profit from an additional legal ground to process special categories of data. If provided for by Member State law, such applications may also be developed within a regulatory sandbox.

FRT systems, which are classified as high-risk, will be required to be designed and developed with humans in mind. As such, they must have a human-machine interface, which allows the human overseer to correctly interpret the outputs, avoid automation bias, use or not use the outputs or change actions and decisions of the system. The human overseer must be able to get a full picture of the capabilities and limitations of the system.

Explainability is only touched upon in Recital 38 of the Proposal and no specific individual rights, such as a right to explanation is currently included. The provisions on explainability in the GDPR will remain untouched. Their scope is, however, severely limited – as is the information to be provided.

Still, the AI Act (in its current version) will significantly increase the design requirements and set an important milestone towards achieving interpretability, traceability, transparency and therefore, ultimately, explainability.

3.4.1. Outlook

The second version of the guidelines will address specific use cases of FRT, which are currently being developed within the consortium. Furthermore, the second version of the guidelines will have to address the recently released proposals for a new liability regime for AI.[199,200] According to the European Commission, the AI liability directive will complement and modernise the EU civil liability framework. For the first time, specific liability rules for damage caused by AI-systems will be introduced. The directive introduces a “presumption of causality” and facilitates access to evidence.[201] Additionally, the new product liability regime will also apply to defective AI systems.

[199] COM (EU) Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM 2022/0302, 496 final.
[200] COM (EU) Proposal for a Directive of the European Parliament and of the Council on liability for defective products COM 2022/0302 495 final.
[201] COM (EU) Questions & Answers: AI liability Directive (available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5793, accessed on 04.10.2022) 1.