Biometric Data, De-identification and the GDPR

E. Kindt
Cost1206
Training school
2017
Overview

Introduction

1. Definition of biometric data
2. Biometric data as a new category of ‘sensitive data’
3. De-identification
4. Specific obligations for biometric data: DPIA and DPbD
5. Other new obligations: Biometric data and scientific research

Conclusions
Introduction

- Legal framework on data protection under revision

- General Data Protection Regulation published in O.J. 4.5.2016 entering into effect on 25.5.2018

- Biometric data addressed

- Additional guidelines on de-identification
Introduction

REGULATIONS

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)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right.

Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the
Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of


(3) Opinion on the draft Legislative Act of 15 December 2015, C 352/30/EU.

4.5.2016 Official Journal of the European Union L 119/1
Introduction


DIRECTIVES

DIRECTIVE (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 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 2008/97/JS

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION.

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Committee of the Regions (1),

Acting in accordance with the ordinary legislative procedure (9),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on, the protection of natural persons with regard to the processing of their personal data, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) The free flow of personal data between competent authorities for the purposes of the prevention, investigation,
1. Definition of biometric data

Article 4

(...)

(14) ‘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;

(...)

- (c) E. Kindt
1. Definition of biometric data

**Personal data : Art. 4.1:**

1. “any information” e.g., voice, but also in template form, ....
2. “relating to”
3. “an identified or identifiable” e.g. by controller or any third party
4. “natural person”

*identifiable natural person* is...

**Data subject**

one who can be identified, directly or indirectly, ....

---

**Art. 4.1 General Data Protection Regulation :**

‘... 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,’
1. Definition of biometric data

Recital 51

(…) The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. (…)
2. Biometric data as a new category of ‘sensitive data’

Article 9

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. (…)
2. Biometric data as a new category of ‘sensitive data’

Exceptions to the prohibition of processing
2. Ten Exceptions to the prohibition

(a) the data subject has given explicit consent (...);

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) (...) vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (...)

- (c) E. Kindt

KU LEUVEN
CENTRE FOR IT & IP LAW
2. Ten Exceptions to the prohibition

(...)

(d) (...) legitimate activities (...) by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition (...)

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) (...) necessary for the establishment, exercise or defence of legal claims (...);

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
2. Ten Exceptions to the prohibition

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or (…) contract;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard (…)
2. Ten Exceptions to the prohibition

‘sensitive data’

(...)

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
2. Biometric data as a new category of ‘sensitive data’

‘sensitive data’

(...) 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

e.g., Art. 9.2(a) or 9.2(h) and art. 9.4 relevant for AAL
2. Biometric data as a new category of ‘sensitive data’

Consequences:

- Different kinds of ‘biometric data’?
- Distinction between images and data resulting from specific technical processing
- Distinction between biometric data used for uniquely identifying and for verification
3. De-identification ≠ anonymization

Recital 51

(...) The principles of data protection should therefore not apply to anonymous information, (i) namely information which does not relate to an identified or identifiable natural person or (ii) to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.’ (numbers added)
3. De-identification ≈ pseudonymisation

Recital 51

(...) Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
3. De-identification

Recital 51

(…) 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. (…)
3. De-identification

Recital 29

In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.
4. Specific obligations for biometric data: DPIA

Article 35.1

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)

- (c) E. Kindt
4. Specific obligations for biometric data: DPIA

Article 35.3
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
   (a) 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), (...)

- (c) E. Kindt
4. Specific obligations for biometric data: DPIA

Article 35.7: The assessment shall 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;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(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.
4. Specific obligations for biometric data: DPIA

Article 35.7: The assessment shall 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;

Art. 4.2 General Data Protection Regulation:

'... any operation (...) performed on 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. Specific obligations for biometric data: DPIA

Article 35.7: The assessment shall contain at least:

(a) (…) where applicable, the legitimate interest pursued by the controller;

(b) where applicable, the legitimate interest pursued by the controller;

Art. 6 General Data Protection Regulation:

1. Processing shall be lawful only if (…)
(a) the data subject has given consent (…);
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) 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;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (…) shall not apply to processing carried out by public authorities in the performance of their tasks. (…)
4. Specific obligations for biometric data: DPIA

Article 35.7: The assessment shall contain at least:
(a) (...)
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

See Art. 52 of the Charter of Fundamental Rights of the European Union
Interference only if proportionate i.e., relevant, effective
and necessary in a democratic society i.e. no other means
4. Specific obligations for biometric data: DPIA

Article 35.7: The assessment shall contain at least:

(...)

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;

See in particular the Charter of Fundamental Rights of the European Union
Art. 7 and 8, but also dignity, free movement, non-discrimination, …
Fundamental right to privacy?

Right to Privacy – ECtHR - the notion of one’s “private life” is “a broad term not susceptible to exhaustive definition”

determined from case to case, depending on facts and circumstances

“covers physical and psychological integrity of a person”

“can embrace multiple aspects of the person’s physical and social identity”

“protects a right to personal development”

“right to establish and develop relationships with other human beings and the outside world”
Interference with right to privacy?

ECtHR /ECJ

• In case of surveillance
• In case of bulk storage and retention of telecom traffic data without appropriate safeguards
• In case of lack of appropriate access control to medical data
• ....
4. Specific obligations for biometric data: DPIA

Article 35.7: The assessment shall contain at least:

(a) (...)

(b) (...)

(c) (...)

(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.
4. Specific obligations for biometric data: DPIA

Example/exercise: AAL and DPIA:

(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;

Processing operations:
- Collection of biometric data (images, sound) and other personal data (behavior, habits, living environment, social relations, of AP, IC, relatives, visitors) (to be completed)
- Storage on platform (cloud?) with service provider
- Transmission to IC, third parties (emergency team) (to be completed)

Purposes:
- Emergency intervention by health practitioners (?) information to IC, social interaction, control of medication (to be completed)
4. Specific obligations for biometric data: DPIA

Example/exercise: AAL and DPIA:

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

Proportionality:
limitation of rooms monitoring; hours per day; limited to specific type of data (camera vs sensor for fall detection?); (to be completed)

Necessity:
all other means (not breaching privacy) to reach each of the objectives (misbehavior in care centres; fall detection; social interaction, (to be completed) should be exhausted
4. Specific obligations for biometric data: DPIA

Example/exercise: AAL and DPIA:

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

Risks: privacy and data protection
Surveillance;
Re-use/Abuse of the personal data (use for other purposes then originally intended e.g., to restrict medical reimbursements or medical care, (to be completed)
Access to unauthorized persons (to be completed)
Risks: other rights: dignity (social visits/interaction replaced by robots? (to be completed); discrimination (to be completed);
4. Specific obligations for biometric data: DPIA

Example/exercise: AAL and DPIA:
(d) the measures envisaged to address the risks, (…)

Various types of image redaction for pseudonymisation (non-continuous) transmission upon incidence only
Transmission and redaction depending on the context and the receiver (IC, emergency, etc)
Limitation of collection of (biometric) data: can you do with less data?
Security for transmission and storage
Restricted access
Timely deletion/limitation of storage up to (to be completed)

and this for each purpose (!)
4. Specific obligations for biometric data: DPIA

Article 35 (…)

8. Compliance with approved codes of conduct (…) by the relevant controllers or processors shall be taken into due account in assessing the impact (…)

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, (…)

10. Where (…) a data protection impact assessment has already been carried out as part of a general impact assessment (…) paragraphs 1 to 7 shall not apply (…..)

11. Where necessary, the controller shall carry out a review to assess (…) when there is a change of the risk represented by processing operations.
4. Specific obligations for biometric data: DPIA

Article 36
Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller (…)
4. Specific obligations for biometric data: DPIA

How? See guidance by national DPAs (e.g., French DPA)
4. Other new obligations: DPbD

Previous developments: PETs

PETs: a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing functionality of the information systems (European Commission, 2007)
In Europe: Privacy Enhancing Technologies

…it also became clear that PbD can play an important role for enhancing the rights of the data subject (a priori safeguard).

“...a more positive solution is to design and develop ICT in a way that respects privacy and data protection...”

Widespread risks and failures [...] particularly when they entail the misuse or breaches of personal data exposing the privacy of individuals, are likely to endanger user trust in the information society (EDPS, 2010)

PbD empowers the user by...

“eliminating/reducing personal data, preventing unnecessary and/or undesired processing or offering tools to enhance individuals' control over their personal data” (EDPS, 2010)

‘Users of ICT services are not in a position to take relevant security measures by themselves in order to protect their own or other persons’ personal data.’ (Art. 29 WP, 2009)
4. Other new obligations: DPbD

Article 25 - Data protection by design and by default

1. Taking into account the state of the art, 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, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement 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 this Regulation and protect the rights of data subjects.
4. Other new obligations: DPbD

**Article 25 - Data protection by design and by default**

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, **only personal data which are necessary for each specific purpose of the processing** are processed. That obligation applies to the **amount of personal data collected**, the extent of their processing, the period of their storage and their accessibility. 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.
In Canada: PbD

The concept of Privacy by Design could be represented as a trilogy of elements:

- Information Technology
- Accountable Design and Architecture
- Business Practices
- Regulation

Cost1206 – Training School – 13-16 Febr. 2016 - (c) E. Kindt
Biometric processing takes place in border control in order to authenticate that the holder of the passport is its rightful owner.
Case study I: Biometric Processing

Possible impact on privacy:

• Biometric processing entails risks to privacy, such as misuse or mismanagement of biometric data, tracking, identity theft that harm the confidentiality and integrity of data.

• Is it then legitimate to employ biometric technologies for this purpose? How can PbD contribute to reduce the impact on privacy?
Case study I: Biometric processing

• The processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 7 of Directive 95/46/EC.

• Fingerprints have been integrated in passports in compliance with the EU Council Regulation 2252/2004 of 13 December 2004. It is thus a legal obligation (Art. 7c)
Case study I: Biometric processing

PbD entails to impose technical measures in the design of the authentication system:

• No central storage of biometric data.

  **Art 29WP view:** “Any central database would increase the risks of misuse and misappropriation. It would also intensify the dangers of abuse and function creep. Finally, it would raise the possibilities of using biometric identifiers as 'access keys' to various databases, thereby interconnecting data sets”.

• A distributed storage (e.g. on a smartcard) is preferred. Biometric data in data subject’s possession.

• **To preserve confidentiality of data** appropriate cryptographic techniques to be employed.
Case study I: Biometric Processing

Council Regulation 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

The storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. (Art. 1)

Additional technical specifications for passports and travel documents relating to the following shall be established: [...] technical specifications for the storage medium of the biometric features and their security, including prevention of unauthorised access (Art. 2b)

The designation of the authorities and bodies authorised to have access to the data contained in the storage medium of documents is a matter of national legislation… (Rec. 4)
5. Biometric data and scientific research

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. (…)

- (c) E. Kindt
5. Biometric data and scientific research

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

(…) Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
Conclusions

• Biometric data are in most cases always personal data
• Not all ‘biometric data’ is biometric data under the GDPR
• Only some biometric data is sensitive
• If processing of biometric data which is sensitive and on a large scale, a DPIA is needed - but also if present high risk, in case of profiling, and monitoring in public spaces on large scale
• Biometric data for research: safeguards needed
Thank you for your attention

Questions ? Comments ?

Additional questions: mail to Els.kindt@law.kuleuven.be