

A legal obligation to protect biometric information

Els J. Kindt, Biometric Law Lab (biometriclawlab.org) - RADL
KU Leuven, Belgium – Universiteit Leiden, the Netherlands
EAB – 14 October 2026

This presentation is partially funded by the European Union's Horizon Europe research and innovation programme under the grant Agreement No 101308502 (DEFORM) and the Norwegian Research Council funded Project SALT.



Overview

- Biometric data will in most/many cases be personal data
- Recent legislation, DPA guidance and case law
- Obligation to protect biometric data as ‘sensitive’ personal data

Conclusions

GDPR and Personal data (1/2)

- Concept ‘Personal data’: Definition in Art. 4 (1) GDPR (same in LED (Art.3(1)):

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);

(….)

- Guidance:
  - *Type* and *format* of info *not relevant* (image, sound, etc) - Includes information *in whatever form* (e.g. stored in binary format) (pp. 7-8) – ‘relating’ can be by content (‘about’), purpose or result (‘impact’)
  - ‘scope of data protection rules should not be overstretched’ < > ‘But, unduly restricting the interpretation of the concept (…) should also be avoided (p. 5)

See Art. 29 WP Opinion 4/2007 on the concept of personal data (WP 136)

(….)

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;

GDPR and Personal data (2/2)

- Rec. 26 GDPR: '(….) To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, (…) 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 (…), 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.

  The principles of data protection should therefore not apply to *anonymous information, namely information which does not relate to an identified or identifiable natural person* or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. (…).'

Recent legislation : GDPR, AIA, Dig. Omnibus

- Biometric data : Art. 4 (14) GDPR (2016) : ‘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’ (same definition in LED)

- Biometric data : Art. 3 (34) AIA (2024) : ‘means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data’

Biometric data as sensitive/high-risk/forbidden

- ‘Sensitive’: Processing of biometric data for the purpose of uniquely identifying : forbidden, safe (10) exceptions (Art. 9 GDPR 2016)

(compare with art. 10 LED 2016) – (Prop. Dig. Omnibus for GDPR and LED : **not including verification if under sole control** - IATA coalition (Oct. 2026))

- High-risk: Remote biometric identification systems (not verification), AI systems for categorization and AI systems for emotion recognition (Annex III.1 AIA 2026)

- Forbidden: Use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for law enforecement safe if strictly necessary for 3 objectives : Art. 5 (h) AIA 2026

Biometric data, bias detection and training

- Dig. Omnibus on AI (2026/1744) : new art. 4a in AIA:

'Article 4a

Processing of special categories of personal data for bias detection and correction

1. To the extent strictly necessary to ensure bias detection and correction in relation to high-risk AI systems in accordance with Article 10(2), points (f) and (g), of this Regulation, providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable, all the following conditions shall be met in order for such processing to occur:

(a) the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;

(b) the special categories of personal data are subject to technical limitations on the re-use of personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation;

(c) the special categories of personal data are subject to measures to ensure that the personal data processed are secured and protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and to ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations;

(d) the special categories of personal data are not transmitted, transferred or otherwise accessed by other parties;

(e) the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first; and

(f) the records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

2. Providers and deployers of other AI systems and models and deployers of high-risk AI systems may exceptionally process special categories of personal data to the extent that:

(a) such processing is strictly necessary to ensure bias detection and correction in view of possible biases that are likely to affect

DPA Guidance



Pieter Breugel the Elder
Tower of Babel – circa 1568

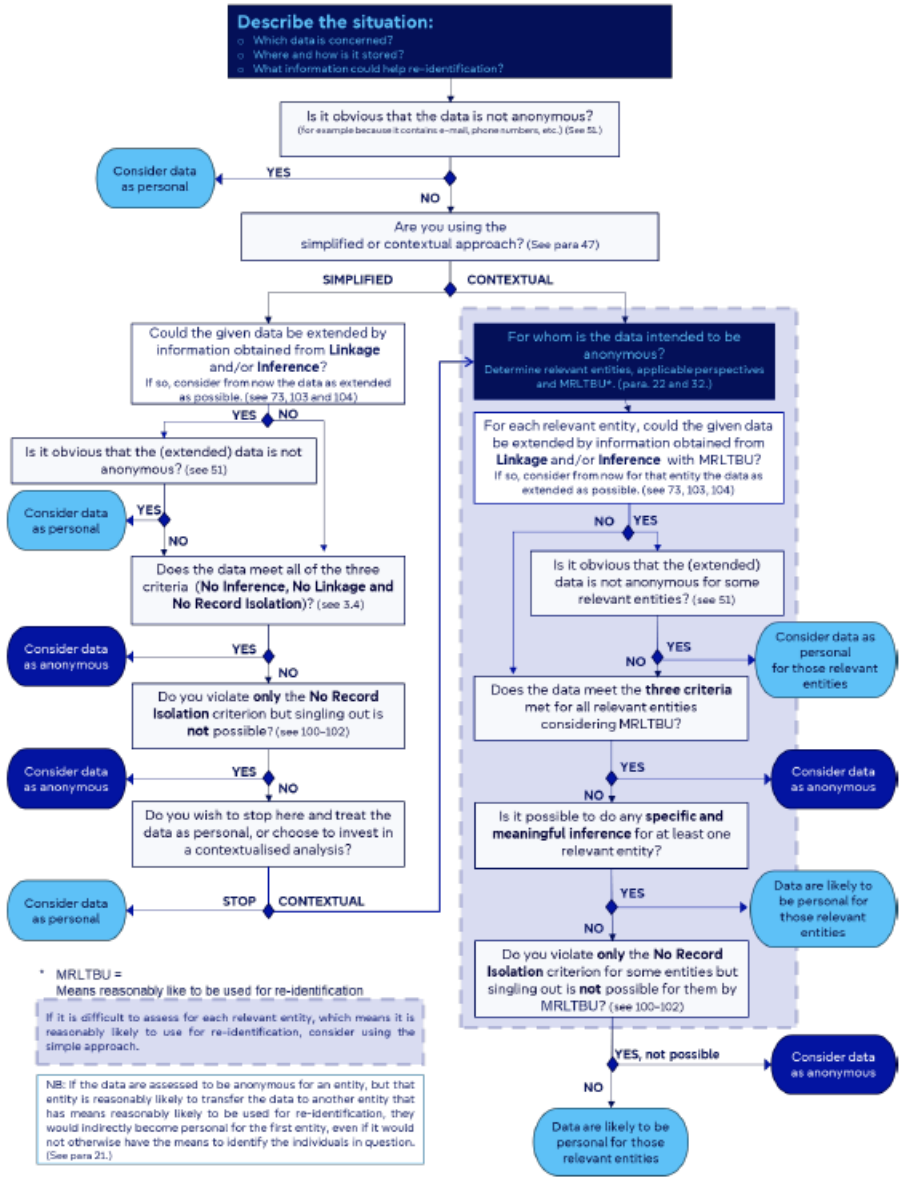
- **Anonymization >> GDPR does not apply**

  "removing directly identifying elements in itself is not enough (…). It will often be necessary to *take additional measures to prevent identification*, once again *depending on the context and purposes* of the processing for which the anonymised data are intended." (italics added) - Art. 29 Working Party Opinion 5/2014 on Anonymisation techniques 2014 (WP216)

  EDPB, (draft) Guidelines 02/2026 on Anonymisation, 7.7.2026, 34 p.
  (public consultation until 30.10.2026)
  No Record Isolation, No Linkage and No Inference

Several key factors to assess (amount of information, detail of attributes, ….
Assessment can take a simplified or contextual approach

This flowchart has been developed as a support tool for organisations intending to anonymise data. In a simplified manner, it presents one way of how the assessment could be done in line with the guidelines.



EDPB, (draft) Guidelines 02/2026 on Anonymisation, 7.7.2026, p.33

DPA Guidance

- Pseudonymization >> GDPR applies !
  - Reducing or transforming information as to make it relate to only *identifiable* persons (not directly identifiable unless with additional information)
  - art. 4(5) GDPR: definition : requires that (i) additional information shall be kept separately ànd (ii) technical and organizational measures
- For scientific research: obligation to protect : obligation of data minimization and additional safeguards (Art. 89 GDPR) >> hence, pseudonymous or anonymous data if possible

Case law

- Breyer case (C-582/14): dynamic website visitors IP address : logged for security : German courts: issue : 'identifiable': objective or relative criterion ?
  - Adv. General: if identification *is prohibited by law* or practically impossible because of disproportionate efforts (§68)
  - Court : '… it is *not required* that all the information enabling the identification of the data subject *must be in the hands of one person*.' (§43)
  - ' in particular, in the event of cyber attacks *legal channels exist* so (…) that (…) can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.' (§47)
- Broad scope was maintained in other cases (e.g., C-579/21 and C-604/22)
- e.g. Taxa 4x35 facing fine of 160,000 euro imposed by Danish DPA for insufficient anonymization ('mere' deleting name of taxi users) (2018)

Case law



Pieter Breugel the Elder
Tower of Babel – circa 1568

- European Data Protection Supervisor (EDPS) v SRB (C-413/23 P), 4.9.2025 :

(indirect) discussion about concept of personal data (objective or relative criterion ?)
and obligation to inform

- Case-law of Breyer is upheld ((§91)
- Court : '… the relevant perspective for assessing (…) identifiable depends, in essence, on the circumstances of the processing of the data in each individual case' (§100)

While:

- '(…) in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, (…) the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.' (§ 85)

- 'pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data (…) in so far as pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.' (§ 86)
- '(…) pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.' (§ 87)

- Case was about *obligation to inform* about the recipients : rests with the controller

Towards a Contextual Concept of Personal Data Under the GDPR: the Commission Moves Forward, the EDPB and EDPS Push Back



By Bartolomé Martín & Manel Benladghem on March 2, 2026

Posted in Court of Justice of the European Union (CJEU), European Data Protection Board, General, General Data Protection Regulation (GDPR)

The European Data Protection Board[1] (EDPB) and the European Data Protection Supervisor[2] (EDPS) adopted on 10 February 2026 a joint opinion (Joint Opinion 2/2026[3]) on the European Commission's Digital Omnibus initiative (described by the Commission as "*a set of technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness*").

Although both bodies welcome (and largely endorse) the Commission's proposals set out in the initiative (subject to certain caveats), the opinion expresses marked unease

DPA Guidance

- Biometric templates ?

In accordance with this definition, measures of biometric identification or their digital translation in a template form in most cases are personal data[11]. It appears that biometric data can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person. In the context of biometrical identification, the person is generally identifiable, since the biometric data are used for identification or authentication/verification at least in the sense that the data subject is distinguished from any other[12].

(…)

Art. 29 WP Working document on biometrics (WP 80) 2003, p. 5

In accordance with this definition, measures of biometric identification or their digital translation in a template form in most cases are personal data[11]. It appears that biometric

'…should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template'

Art. 29WP Opinion 3/2012 on developments in biometric technologies, WP193, p. 4

European Data Protection Supervisor (EDPS) Guidance

- Protected Biometric templates ?

above. Therefore, the use of a biometric identity, instead of the raw biometric fingerprint, enhances the protection of the latter, since it is considered impossible, in technical terms, to extract the fingerprint information directly from the biometric identity as proposed by Turbine. However, due to the fact that the exclusive connection of the biometric identity with a specific person still exists (as only the capture of the fingerprint of the same person could lead each time to the production of the same biometric identity with the use of the same cryptographic algorithm), the biometric identity may lead to the identification of that person, in the same way that the raw biometric element does. In other words, although the biometric identity could not independently lead to disclosure of information relating to a person, it may nevertheless lead to the identification of this person within the framework of the biometric system operation (e.g. during access control) in combination with other personal data kept in the system for the same person (e.g. full name). In this sense, the biometric identity, as it is produced and used by the Turbine project, also constitutes personal data.[7]

See EDPS, 'Turbine' Opinion, 2011, p. 5

>> Hence: Irreversible unlinkable and revocable identifiers: enhances considerably privacy and data protection (but: risk of re-purposing, identification, … remains) (!)

- Likely same for use of fully homomorphic encryption
- dpby design obligation ?

DPA assessment : e.g., Datatilsynet (2025)

- Protected Biometric templates :

(…) Secure processing: The plaintext template is secured by a transformation process using the transformation key, followed by an encryption process using the homomorphic encryption key. This process results in the generation of a protected template. The protected template is then sealed using the sealing key. This ensures the integrity of the protected template. (…) (p. 9)

- Personal data ?

‘(…) We argue that while homomorphic encryption and protected templates make the information incomprehensible to other parties without the encryption key, this does not necessarily guarantee anonymity. As long as the encryption key can be used to link the template to a real person, we contend that it falls within the definition of personal information and therefore the GDPR applies. (…) (p. 3)
(….

Datatilsynet, Securing Digital Identities. Biometric data and protected templates in eID solutions, 2025, 24 p.

Legal Obligation to Protect Biometric Data = Obligations to use BPTs ?

>> 'Data Protection by Design and by Default' (Art. 25 GDPR)

- 'shall implement appropriate technical and organisational measures, *such as pseudonymisation'*

- 'designed to implement data-protection principles, such as *data minimisation*' 'in an effective manner'

- Art. 25.3: 'An appropriate *certification mechanism*' may be used to demonstrate compliance

>> Data Protection impact assessment (DPIA)(Art. 35 GDPR) and Fundamental Rights impact assessment (FRIA) for high-risk systems (Art. 27 AIA) :

>> Controller and processor shall implement 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…)' (Art. 33 GDPR/see also Art. 15 AIA)

Case-by-case assessment

Key-issue :

>> ‘all the means reasonably likely to be used’ ? ; context ?

- on voluntary basis or e.g., by court order,….

Case-by-case assessment : Quid if BPT remains part of an identification system ? Example:

- Country database (db) with one way encrypted biometric information of individuals who assisted with regime A
- Regime B overtakes country /country enters into war
- Suspects of assisting regime A in the db ?
  - GDPR: Cost, time and technology available to re-identify persons ?
    - Access to facial image of suspect (yes) and access to biometric ‘comparator’/algo (possibly yes) would allow re-identification

>>one-way encrypted biometric information would remain personal data (with knowledge of the key : ‘all means reasonably likely to be used ?’)

Purposes - context ?

- When used in identification system ?

  >> Can hardly say it is not personal data

  - Cfr. Art. 29 WP Working document on biometrics (WP 80) 2003 – also EDPS, Turbine opinion 2011 - ….

- When images are used for research purposes ?

  e.g. For training ? Will not be used to (re)identify /identification system

  - Pro memorie: Research : Needs appropriate safeguards (‘technical and organisational measures’ ‘pseudonimisation’ ‘anonymisation’ if can meet research objectives) (see Art. 89 GDPR)

>> Pseudonymous biometric information for research purposes (eg public db) remains personal data

>> Hence, context could be important, but not determining - contexts may also change outside the control of the entity and individual (‘re-purposing’ ‘function-creep’)

e.g., social media images scraped and used by Clearview AI for offering identification tool to LEA in numerous countries

Conclusion (1/2)

- Strict criteria for anonymous data ; if not fulfilled, pseudonymous data
- Data protection by design and by default and security obligations (!)
- BPT - one way encrypted biometric (protected) information(i.e. revocable and unlinkable (cfr ISO standard)) : enhances data and privacy protection
- Use of standards: responsibility of controller – form of self-regulation – but: part of certification mechanism ?

Conclusion (2/2)

- GDPR /AIA protection to BPT - one way encrypted biometric (protected) information ?

  - In identification systems: will be considerd as (pseudonymous) personal data – not anonymous data
  - If used/processed for uniquely identifying: is biometric data and ‘sensitive’ – art. 9 GDPR applies
  - If used in ‘remote’ identification system by law enforcement in publicly accessible places: forbidden (Art. 5 AIA) ; all other systems: high risk (Art. 6 AIA)

  - In research context/for training: likely remains (pseudonymous) personal data – this does not prevent use for research (!) – depending on the context, may in (exceptional) cases, for some entities, become anonymous ??

Resources and more reading (selection)

- General Data Protection Regulation, 2016 (all languages), AIA, 2024 and Dig. Omnibus on AI (2026)

- Guidelines and Opinions :

  - Art. 29 WP Working document on biometrics (WP 80) 2003
  - Art. 29 Working Party Opinion 3/2012 on developments in biometric technologies (WP193)
  - Art. 29 Working Party Opinion 5/2014 on Anonymization techniques 2014 (WP216)
  - Datatilsynet, Securing Digital Identities. Biometric data and protected templates in eID solutions, 2025, 24 p.
  - EDPB, (draft) Guidelines 02/2026 on Anonymisation, 7.7.2026, 34 p. (public consultation until 30.10.2026)

- Scholarship:

- E.J. Kindt and C. Jasserand, 'Chapter 3: A legal obligation to protect Biometric Information: A Brief Analysis' in V. Krivokuca Hahn, M. Gomez-Barrero, A. Ross and S. Marcel, *Handbook of Biometric Template Protection- Motivation, Methods and Metrics*, Springer Nature, Singapore, 2026, pp. 45-75
- B. Sumer, N. Menéndez González, A. Elbi, C. Jasserand, J. Czarnocki and E. J. Kindt, 'Chapter 5: AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Biometric Data Regulation ?' in K. Prifti e.o., (eds)., *Digital Governance: confronting the challenges posed by Artificial Intelligence,* LAIR conference book, The Hague, The Netherlands, T.M.C. Asser Press, in cooperation with Springer, Heidelberg, 2024, pp. 165-181

Thank you for your attention !



If questions: els.kindt.radl@telenet.be

This presentation was partially funded by the European Union's Horizon Europe research and innovation programme under the grant Agreement No 101308502 (DEFORM) and the Norwegian Research Council funded Project SALT.



The presentation reflects only the author's views and the sponsors are not liable for any I

Use that may be made of the information contained herein