PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation.

BIOMETRICS

Biometrics in ICT research and innovation

Alessandro Ortalda, Carlotta Rigotti, Andrés Chomczyk Penedo, Paul De Hert (VUB)

This part of the Guidelines was reviewed by Stefano Leucci (European Data Protection Supervisor), Ernestina Sacchetto (University of Turin); Catherine Jasserand-Breeman (KU Leuven) and Lydia Belkadi (KU Leuven).

This was finally validated by Prof. Ger tVermeulen, former privacy commissioner at the Belgian Data Protection Authority and a former member of the European Data Protection Board's BTLE subgroup (Borders, Travel and Law Enforcement)

Basque Data Protection Agency.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains

1 Introduction and scope

Research activities may sometimes involve the processing of biometric data, which requires researchers and research institutions acting as data controllers or processors to address data protection requirements. Since biometric data enjoy a special protection regime under the EU regulatory framework, researchers working with biometric data should comply not only with the general data protection requirements and the specific requirements provided in article 89 of the European General Data Protection Regulation (GDPR) related to research activities[1], but they should also implement additional safeguards tailored to the specificities of biometric data and/or biometric processing (see "Data protection and scientific research" within Part II, section "Main concepts" of these Guidelines).

The following guidelines provide guidance on how to comply with the legal obligations enshrined in the European data protection regime. In particular, the document is concerned with ICT research activities that include the development of ICT systems employing biometric data. The authors acknowledge that nowadays it is common for such systems to adopt artificial intelligence technologies. Dedicated guidelines for artificial intelligence can be found in Part III of these Guidelines.

This Part VI is addressed to ICT research institutions working with biometric technology as data controllers, including not only the researchers, who might not be aware of the legal obligations coming from their research activities, but also other concerned parties such as legal departments or ethical committees, which might be more versed on legal aspects but not necessarily on the special data protection regimes applicable to biometric data and research activities. To ensure both, audiences can easily access the contents of the guidelines. The document attempts to strike a balance between technical details (both regarding ICT and biometric technology, and data protection law) and general accessibility.

2 Definitions

2.1 Special categories of personal data

Before defining biometric data, it is necessary to look at 'special categories of personal data', also commonly known as 'sensitive data'. Indeed, article 9.1 GDPR clusters biometric data (or, at least, some of them; see section 2.2 "Biometric data") in this broader group:

Special categories of personal data

[1] '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' (2016).

Data revealing racial or ethnic origin
Data revealing political opinion
Data revealing religious or philosophical beliefs
Data revealing trade union membership
Genetic data
Biometric data (for the purpose of uniquely identifying natural persons)
Data concerning health
Data concerning a natural person's sex life or sexual orientation

By default, Article 9 GDPR prohibits the processing of special categories of personal data, unless one of the exceptions listed in article 9.2 GDPR occurs. One of these exceptions occurs when the "processing is necessary for [...] scientific or historical research purposes".

It is worth noticing that, in order to be compliant, it is not enough for a processing of special categories of personal data to meet one of the exceptions listed in article 9.2 GDPR. In addition to that, and before the processing begins, the data controller shall identify an appropriate legal basis for the data processing (see section 3.2.3 "Identify the most appropriate legal basis")[2].

Data controllers should also be aware that as per article 9.4 GDPR, Member States can introduce further conditions and apply additional requirements and limitation regarding the processing of genetic data, biometric data or data concerning health. Thus, data controllers willing to process these special categories shall always check if there are specific national requirements that apply. Further information can be found in the National Reports produced by the PANELFIT consortium (which can be accessed at https://www.panelfit.eu/national-reports/).

Although certain data do not amount to special categories of personal data by themselves, when employed in conjunction to other data they might amount to special categories of personal data. For instance, the address and mother tongue of a person are not special categories of personal data. However, when name, birthplace and other data of the data subject is attached to the dataset, the combination might reveal enough information to identify racial or ethnic origin of the data subject with a reasonable degree of certainty. In this scenario, data should be subject to the same requirements and limitation of special categories of personal data even if they are not by themselves.

[2] See also Ludmilla Georgieva and Christopher Kuner, 'Article 9. Processing of Special Categories of Personal Data', in *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, United Kingdom: Oxford University Press, 2019), 376–77.

Dataset 1	**Dataset 2**
Address: Washington D.C.	Address: Washington D.C.
Mother tongue: French	Mother tongue: French
	Name: Seydou Kablan Bakayoko
	Birthplace: Abidjan
	Other known language: Cebaara, English
	Primary school: École Konan Raphael, Abidjan
Dataset 1 does not provide information about the racial or ethnic origin of the data subject	*The information provided by Dataset 2 could be considered enough to reveal the racial or ethnic origin of the data subject (with a reasonable degree of certainty)*

It should be noted again that data should satisfy a reasonable degree of certainty. This degree of certainty is contextual and needs to be evaluated on a case-by-case basis.

2.2 Biometric data

The term 'biometric data' is defined in Article 4.14 GDPR. Accordingly, biometric data are "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person". The definition suggests that for personal data to be considered 'biometric' they need to satisfy four *criteria*[3].

First, they need to amount to 'personal data', defined in Article 4.1 GDPR as "information relating to an identified or identifiable natural person". Second, they require 'specific technical processing' to extract the information from the raw data source (for instance, extracting facial features from a picture to measure them). Recital 51 of the GDPR states that 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". Thus, biometric data short of 'specific technical processing' do not amount to biometric data in the context of the GDPR[4]. However, even when data do not amount to biometric data

[3] On the analysis of the definition provided in the GDPR, see C. Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data', *European Data Protection Law Review* 2, no. 3 (2016): 297–311, https://doi.org/10.21552/EDPL/2016/3/6.

[4] Scholars debate if this should be applied as well to technical processing that are prerequisite for identification, such as mere storage in databases. See for instance, Kindt, *Having yes, using no? About the new legal regime for biometric data*, Computer Law and Security Review, 34, 2018, pp. 523-538. For

at a certain stage, they might be part of a data processing that makes them biometric data at a later stage. For instance, a database might host pictures that will be used to perform biometric identification through specific technical processing at a later stage (thus, not amounting to biometric data yet). Imagine a scenario in which said database is directly linked to the system that performs the biometric identification (see also section 2.3 2Biometric System"). In this case, unauthorized parties might exploit this link to access biometric data. For instance, they might exfiltrate the (non-biometric) pictures hosted in the database and, after having violated the system that performs the biometric identification, they might run the picture through it and perform the biometric identification, thus getting access to the biometric data. In this scenario, a weak security ensures that external parties can obtain biometric data even if these biometric data have yet to exist. Data controllers should approach this from a risk-management perspective. If they cannot guarantee appropriate risk mitigation to the non-biometric data (i.e., exploitation risks) then these datasets should be considered as biometric ones and be subject to all the legal requirements, even if they don't fulfil – by themselves – the criteria for being considered biometric data.

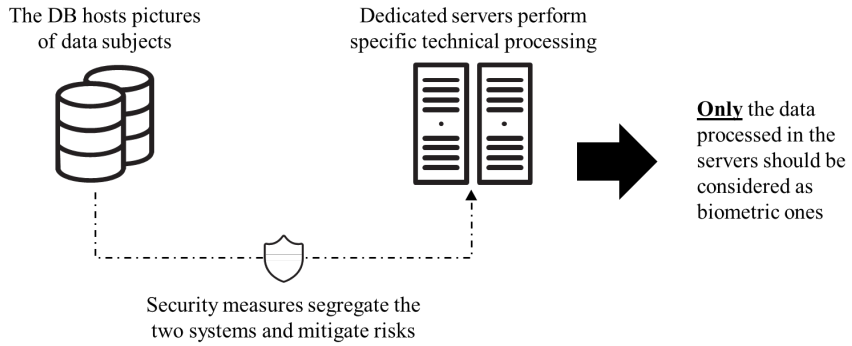


Figure 31 Biometric data scenario 1

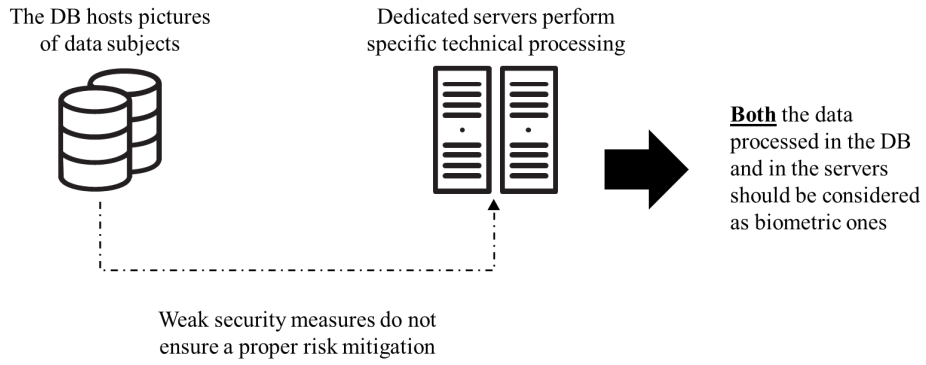


Figure 32 Biometric data scenario 2

The third *criterion* pertains to the features of the data subjects that are captured through the specific technical processing mentioned above. These features can be 'physical', 'physiological' or 'behavioral', and are different from accidental qualities such as the

an analysis of the issues around format other than photographs see Andras Nautsch *et al.*, Preserving privacy in speaker and speech characterization, Computer Speech & Language, 58, 2018, p. 445.

address of the data subject, its location at a given moment, employment data, etc. The fourth and last *criterion* states that for personal data to be considered biometrics they need to allow or confirm the unique identification of a natural person. Indeed, biometric data do not necessarily uniquely identify individuals *per se*. For instance, biometric data could be used to distinguish between humans and animals, or between men and women[5]. However, differently from other identifiers such as names or identification codes, the processing of biometric data does not return a clear-cut identification. Rather, it allows the identification of individuals with a certain degree of probability. According to an established view, data should be considered as biometric ones "even if patterns used in practice to technically measure them involve a certain degree of probability"[6].

2.3 Biometric system

The present chapter defines 'biometric system' as any system capable of uniquely identifying natural persons (with a certain degree of probability) by performing specific technical processing relating to the physical, physiological, or behavioral characteristics of the natural persons[7]. The definition covers both all-in-one systems that perform all the steps (e.g., data acquisition, data elaboration, data storage, etc.) or clusters of systems each performing individual steps (e.g., a network of data capturing module based on a camera, a biometric mapping software and a database for storage). When a system performing one or more individual steps (hereinafter, "system X") does not in itself qualify as a biometric system – as per definition above – but is nevertheless part of a cluster of systems that include biometric ones, system X should be considered as a biometric system unless it can be demonstrated – possibly through documented evidence – that it does not process biometric data and that risks are effectively mitigated (e.g., the risk of unauthorized third parties using system X to gain access to another system directly linked to system X where biometric data are processed).

Often, biometric systems rely on artificial intelligence technology. The use of such artificial intelligence poses further data protection risks that data controllers need to address. Therefore, it is advisable to consult Part III of these Guidelines.

2.4 Types of biometric data

As already mentioned, different biometric data may be derived from different characteristics a natural person exhibits – physical physiological, behavioral. The present section illustrates these different types of biometric data. The following taxonomy is not established as a standard and certain types of biometric data might be

[5] See for instance '14 Misunderstandings with Regard to Identification and Authentication' (Agencia espanola proteccion datos, European Data Protection Supervisor, June 2020), 3.

[6] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data', 2007, 8. See also Article 29 Data Protection Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies', 2012, 6.

[7] Although the International Organization for Standardization produced a detailed vocabulary of terms related to biometrics, which include the definition of 'biometric system', the other of the present document prefer to adopt a definition built on the provisions of the GDPR. See International Standardization Organization and International Electrotechnical Commission, 'ISO/IEC 2382-37 - Information Technology - Vocabulary - Part 37: Biometrics', 2017.

categorized differently by different experts. For example, taxonomies sometimes cluster physiological biometric data into physical biometric data.

2.4.1 Physical biometric data

Physical biometric data can be generated by capturing distinctive bodily features of individuals. The distinctiveness of these features can then be employed as an identifier. Some of the most common physical biometric characteristics are fingerprints, hand shape, facial features (such as the roundness of the face, the distance between the eyes, etc.), and iris features.

2.4.2 Physiological biometric data

Physiological biometric data can be generated by observing bodily functions and capturing distinctive patterns associated to them. Some of the most common physiological biometric data are generated from electrocardiograms (ECG), respiration patterns, and electroencephalograms (EEG).

Although physical biometric data is often used as a synonym of physiological biometric data – and *vice versa* – the authors believe a distinction could be beneficial to better frame the discussion, especially considering recent studies on the relation between biometric technology and certain physiological functions, such as neurophysiological ones[8].

2.4.3 Behavioral biometric data

Behavioural biometric data can be generated by observing the behavior of individuals, to identify distinctive patterns in such behavior. Some behaviors are inherent to the individuals – such as gait, or voice – while others require the interaction with specific tools to manifest – such as handwriting, keystroke dynamics, and mouse movement.

Differently from physical biometric data, behavioral biometric data require an observation of the individuals that introduces a time variable in the assessment[9]. It is often contended that, despite being more volatile to momentarily fluctuations and changes through the lifetime, behavioral biometric data have the advantage of being less intrusive and cost effective[10]. However, some scholars have observed that behavioral biometric data might introduce more privacy risks compared to other kinds of biometric

[8] See for instance, Patrizio Campisi and Daria La Rocca, 'Brain Waves for Automatic Biometric-Based User Recognition', *IEEE Transactions on Information Forensics and Security* 9, no. 5 (May 2014): 782–800, https://doi.org/10.1109/TIFS.2014.2308640.

[9] See Roman V. Yampolskiy and Venu Govindaraju, 'Behavioural Biometrics: A Survey and Classification', *International Journal of Biometrics* 1, no. 1 (2008): 81, https://doi.org/10.1504/IJBM.2008.018665.

[10] See Madeena Sultana, Padma Polash Paul, and Marina Gavrilova, 'A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends', in *2014 International Conference on Cyberworlds* (2014 International Conference on Cyberworlds (CW), Santander, Cantabria, Spain: IEEE, 2014), 271–78, https://doi.org/10.1109/CW.2014.44.

data[11], due to their capability to reveal further information on data subjects, sometimes of very sensitive nature such as health condition[12].

2.5 Research activity

The term 'research activity' does not have a clear-cut definition in the legal framework. According to Recital 159 GDPR, "the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research".

The European Data Protection Supervisor (EDPS) identifies the main goal of research activities in "growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests"[13]. Hence, it seems that the mere research of new commercial technology might not amount to 'research activity' under the current legal framework (see section 4.1 "Data protection and scientific research" in document 'Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation').

3 Biometric technology in ICT research and innovation. Guidelines

The following section provides an overview of practical steps that can be taken when developing biometric technologies or when employing such technologies in the context of ICT research and innovation. These steps can help researchers to comply with data protection obligations. The recommendations are applicable to biometric systems regardless of the biometric data they generate and process (for more information see section "Biometric system").

3.1 Design phase

During the design phase, researchers set the stage by identifying goals and needs of the research activity.

3.1.1 Identify the goals, if the activity qualifies as 'research', and the roles of stakeholders

Researchers should first identify the goal of their activity (e.g., to perform a theoretical study, to develop a biometric system, to test an existing one, etc.). This is an important step not only to define the purposes for which personal data will be collected, but also to

[11] See Günter Schumacher, 'Behavioural Biometrics: Emerging Trends and Ethical Risks', in *Second Generation Biometrics: The Ethical, Legal and Social Context*, ed. Emilio Mordini and Dimitros Tzovaras (Springer, 2012).

[12] See for instance Marcos Faundez-Zanuy et al., 'Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health', *Cognitive Computation* 12, no. 5 (September 2020): 940–53, https://doi.org/10.1007/s12559-020-09755-z.

[13] European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research' (European Data Protection Supervisor, 6 January 2020).

help researchers identify if the activity qualifies as 'research' and, consequently, if the specific legal provisions for research activities apply. Article 89.2 GDPR, for instance, introduces several derogations for processing of personal data in the context of research. In particular, the article acknowledges that certain data subjects' rights (right of access, right to rectification, right to restriction, right to object. For more information see "Data Subject Rights" in Part II of these Guidelines) would make it harder or impossible for some research to achieve its goals. Therefore, it provides derogations from these rights when two *criteria* are satisfied. First, the exemption shall be explicitly provided for by Member States or Union law. This means that, in addition to the GDPR provisions, researchers can be exempt from the obligation to comply with such rights only insofar as there are specific legal grounds in a national law or in EU law other than the GDPR (see section "Identify the most appropriate legal basis"). Second, the researchers shall implement appropriate technical and organizational measures to safeguard the rights and freedoms of data subjects, as required by Article 89.1 GDPR. Given the potential compliance impact for the research activity, it is important to assess immediately if the activity qualifies as 'research'.

A correct scoping of the activities is also necessary for researchers to understand the data protection risks linked to the research. For instance, systems to be used in healthcare or law enforcement are likely to require more accurate outcomes than ones employed for leisure activities (such as music streaming services). Since the accuracy of a system might in certain cases be dependent on the quantity of personal data to be processed (e.g., during the training of an AI algorithm), the need for more accuracy might introduce more data protection risks. Researchers should identify with clarity what level of accuracy the system will have to satisfy and define strategies to ensure that such accuracy is reached by introducing the lowest risk level possible, for instance by limiting the amount of personal data processed (see "Data Minimization" in Part II, section "Principles" of these Guidelines).

Last, but not least, researchers need to understand their role and the roles of other actors involved. Researchers have to look at their involvement in the expected data processing to understand if they (i.e., the entity they work for) are the entities with the main responsibilities over the data processing (data controller), if they share the data controller role with other entities (joint controller), or if they process data on behalf of other entities (data processor). Different roles involve different distribution of responsibilities and liabilities.

3.1.2 Confirm the need to process biometric data

As already mentioned, the GDPR prohibits the processing of special categories of personal data – thus including biometric ones – unless specific exemptions apply (see section "Identify the most appropriate legal basis"). Therefore, researchers planning to process biometric data need to be certain that processing them is necessary to achieve the goal of the research activity. For instance, the research goal might be to develop and test a new approach to increase the accuracy of facial features detection systems. In this case, the goal is not to increase the accuracy of uniquely identifying individuals, but only the accuracy of facial features detection. Thus, researchers might rely on computer generated facial images rather than pictures of an existing natural person, removing the need to process biometric personal data. In case of system development, researchers should also consider how the biometric system will process biometric data after its deployment. Researchers are required to implement in advance all the technical and

organizational measures to ensure that any potential risk is mitigated and data processing occurring after the deployment will be performed in compliance with the legal framework.

3.2 Preparation phase

During the preparation phase, researchers lay the foundations of the research by implementing all the preparatory work for the research activity.

3.2.1 Appoint a Data Protection Officer

The Data Protection Officer (DPO) supports the controller or processor to comply with the data protection norms. Article 37 GDPR mandates the appointment of a DPO in five specific cases.

Requirements mandating a Data Protection Officer	
Requirement 1	"The processing is carried out by a public authority or body, except for courts acting in their judicial capacity", Article 37.1 GDPR
Requirement 2	"The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale", Article 37.1 GDPR
Requirement 3	"The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9", Article 37.1 GDPR
Requirement 4	"The core activities of the controller or the processor consist of processing on a large scale of […] personal data relating to criminal convictions and offences referred to in Article 10", Article 37.1 GDPR
Requirement 5	"[T]he controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer", Article 37.4 GDPR

Requirements 1 and 3 are particularly relevant for this document. Requirement 1 is relevant because it is not uncommon for research institutions to be public bodies, as in the case of public hospitals and public universities. When such a scenario applies, Article 37.3 GDPR provides that "a single data protection officer may be designated for several such authorities or bodies". For example, public hospitals might not have appointed a DPO but could rely on the DPO to provide their service. Requirement 3 is relevant as it mentions the processing of special categories of personal data – such as biometric data – as one of the three *criteria* for the compulsory appointment of a DPO. The other two occur when the processing of personal data happens in the context of a core activity and is performed on a large scale. The terms 'core activities' and 'large scale' are not explicitly defined in the GDPR. The Article 29 Working Party (WP29), though, provide interpretative guidance in its Guidelines on Data Protection Officers. Accordingly, core activities are "key operations to achieve the controller's or

processor's objectives"[14], hence excluding supporting or ancillary activities. In the context of ICT research and innovation, this could be understood as any activity directly related to the execution of ICT research and the achievement of ICT innovation, such as in the case of a biometric system development. As for the large-scale *criterion*, WP29 links it to "the number of data subjects concerned – either as a specific number or as a proportion of the relevant population –, the volume of data and/or the range of different data items being processed, the duration, or permanence, of the data processing activity, [and] the geographical extent of the processing activity"[15].

If appointing a DPO is required, this should occur as early as possible. Indeed, Article 39.1(a) GDPR states that one of the responsibilities of the DPO is to inform and advise the data controller during all the steps of the research. Therefore, securing the assistance of a DPO at the earliest possible time ensures that the researchers receive adequate guidance on how to address the compliance requirements.

The contacts of the DPO should be published and made available to the data subjects.

3.2.2 Identify the data collection approach

The next step for the researchers is to identify if personal data are going to be collected directly from the data subjects, or indirectly (e.g., other researchers, commercial databases, etc.). While this does not necessarily bind researchers to adopt a particular legal basis (see section "Identify the most appropriate legal basis"), it might influence such decision. For instance, if researchers decide to collect data directly from the data subjects, they might be more favorable toward using consent as the legal basis, since a direct relation with the data subjects is going to be established anyway. Moreover, as per Articles 13 and 14 GDPR, choosing a direct or indirect approach to data collection changes the information that the data controllers need to provide to the data subjects.

Information to be provided to data subjects according to the collection approach		
	Directly	**Indirectly**
The identity and contact details of the controller	☐	☐
If applicable, the identity and contact details of the controller's representative	☐	☐
The contact details of the data protection officer	☐	☐
The purposes of the processing	☐	☐
The categories of personal data concerned		☐
The legal basis for the processing	☐	☐

[14] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ("DPOs")', April 2017, 20.
[15] Article 29 Data Protection Working Party, 21.

If applicable, legitimate interests pursued by the controller or by third parties	☐	☐
Recipients or categories of recipients of the personal data	☐	☐
The intention of the controller to transfer personal data to a third country or international organization	✓	☐
In case of transfer, the existence or absence of an adequacy decision by the Commission, or, where applicable, reference to the safeguards and the means by which to obtain a copy of the data	☐	☐
The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period	☐	☐
The existence of the right to request access to and rectification or erasure of data or restriction of processing concerning the data subject or to object to processing and the right to data portability	☐	☐
In case of 'explicit consent' as legal basis for processing, the existence of the right to withdraw consent at any time	☐	☐
The right to lodge a complaint with a supervisory authority	☐	☐
The source of the personal data, and if applicable, whether they came from publicly accessible sources		☐
Whether the provision of data is a statutory or contractual requirement, or a requirement to enter into a contract, and whether the data subject is obliged to provide the data and the consequences of failure to provide such data	☐	
The existence of automated decision-making, including profiling	☐	☐
In the case of automated decision-making, information on the logic involved, the significance of processing, and its envisaged consequences for the subject	☐	☐

The GDPR acknowledges there might be cases when this information duty might not be applicable and lists exemptions in Article 14.5 GDPR. These exceptions are:

- The data subject already has the information;
- The provision of such information:
    - proves impossible;
    - would involve a disproportionate effort,
    - is likely to render impossible or seriously impair the achievement of the objectives of that processing.

In this regard, it is important to clarify that this exception particularly applies for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in compliance with the conditions and safeguards enshrined in Article 89.1 GDPR.

Besides, in such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

- The controller is required by EU or Member State law to obtain or disclose the personal data; or
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Regardless of how data is collected, the data controller shall take appropriate steps to ensure the data is accurate and up to date (e.g., regular accuracy audit). Collecting data directly from the data subjects might help to lower the risk of inaccuracy (especially regarding behavioral biometric data, which might change over time). Also, the controller shall ensure transparency in every step of the process (see "Lawfulness, fairness and transparency" in Part II, section "Principles" of these Guidelines). For a more detailed explanation regarding the right to information and its nuances, please see "Data Subject Rights" in Part II of this Guidelines.

3.2.3 Identify the most appropriate legal basis

One of the most crucial steps from a data protection standpoint is the identification of the legal basis for the processing of personal data, which are listed in Article 6 GDPR. However, as already mentioned, the processing of biometric data is prohibited and can occur only when specific exemptions apply. These are provided for in Article 9.2 GDPR and are of two types. Those that are immediately valid and applicable, and those requiring additional Union or Member State law before they can be employed to justify a processing of biometric data.

Available legal bases provide by the GDPR to process biometric data	
	Requires additional EU or MS law
Explicit consent	
Employment, social security, and social protection	?
Vital interests	
Activities from associations and other not-for-profit entities	
Data have been published by the data subject	
Legal claims or judicial acts	

Substantial public interest	☐
Health or social care	☐
Health public interest	☐
Archiving, research, and statistics	☐

When one of these exemptions applies, then it is possible for the data controller to select one of the legal bases listed in Article 6 GDPR and process personal data accordingly.

Among the ten exemptions of Article 9.2 GDPR, two are particularly relevant in the present document. The first one is the 'explicit consent' requirement. In the context of biometric data processing, the consent of data subjects shall be 'explicit', meaning that it shall be a clear, specific, and unequivocal statement that the data subjects are consenting to have their biometric data processed for the specific purposes identified by the data controller[16]. For instance, in case of processing of biometric data extruded from pictures, it will not be enough to collect data subjects' consent about the processing of said pictures. The subjects shall be informed that biometric features will be extracted and processed, and explicit consent shall be collected.

Example: Consent vs Explicit consent	
Consent	**Explicit consent**
"Please provide a front-facing picture of yourself, taken in a well-lit environment. The picture will be used to extract biometric features for the purpose of developing a new biometric recognition system."	"A - Please provide a front-facing picture of yourself, taken in a well-lit environment. B - The picture will be used to extract biometric features for the purpose of developing a new biometric recognition system. C - Before sending the picture, please mark the following box to indicate that you are providing your consent as data subject to having your picture processed for the purpose of extracting biometric features to be processed pursuant the purpose described at point B.

[16] The GDPR acknowledges in Recital 33 that it might not be possible to fully identify the purpose of the data processing at the time of data collection and, therefore, that data subjects should be allowed to provide consent to certain "areas of scientific research". The point raised by Recital 33, and a number of interpretative challenges have been investigated in the document 'Issues and gaps analysis on informed consent in the context of ICT research and innovation'.

	Check the box ☐”

When talking about consent in the context of research, it is also important to distinguish between the consent to be a participant in the study, and the consent to have personal data processed. These are two different kinds of consent and shall be collected independently[17]. The research team can rely on a single consent form, provided that the form clearly distinguishes between the two kinds of consent and does not collect them in one single agreement (for more information see document “Issues and gaps analysis on informed consent in the context of ICT research and innovation” at https://www.panelfit.eu/wp-content/uploads/2020/11/D21-Issues-and-gaps-analysis-on-informed-consent-in-the-context-in-ICT-research-and-Innovation.pdf).

Another exemption to the processing of special category of personal data that is relevant for the purpose of this document is the exemption for processing necessary to research activities. The exemption requires to satisfy two *criteria* to make it applicable. First, the processing shall be subject to appropriate technical and organizational safeguards as per Article 89.1 GDPR. Second, there should exist Union or Member States law providing a legal ground for processing in the context of a research activity. This last *criterion* implies that the exemption for research purposes might not be applicable everywhere. Therefore, researchers need to carry out a review of national legislations for all the States where the research is going to be carried out in order to identify if such norms are present (see “Comparative study of national reports” at https://www.panelfit.eu/national-reports/).

3.2.4 Create a repository for supporting documentation

The GDPR requires data controllers not only to comply with data protection obligations, but also to be able to demonstrate their compliance with such obligations and with the principles enshrined in the norm. This means the data controller shall keep appropriate records and documentation pertaining to the data processing and the governance of such processing.

Apart from a limited set of documents that are clearly mandated (such as the record of processing activities required by Article 30 GDPR) it is a duty of the data controller to identify what are the necessary documents to demonstrate compliance. The following tables presents the list of documents mandated by the GDPR with the related location in the text. It should be considered a minimum baseline rather than an exhaustive checklist. Indeed, although not mandated, additional documents might be necessary to demonstrate compliance (e.g., reports of prior consultations with supervisory authorities, description of implemented technical and organizational measures, etc.)

Documentation: checklist

[17] See European Data Protection Board, ‘Guidelines 05/2020 on Consent under Regulation 2016/679’, May 2020, 30; European Data Protection Board, ‘Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation’, 2019.

1	Personal data protection policy	Article 24.2
2	Privacy notice	Articles 12, 13, 14
3	Data Retention Policy	Articles 5, 13, 17, and 30
4	Data Retention Schedule	Article 30
5	Record of processing activities (if applicable)	Article 30
6	Consent form (if applicable)	Articles 6, 7, 9
7	Data processing agreement with suppliers	Articles 28, 32, 82
8	Data Protection Impact Assessment	Article 35
9	Appointment of an EU representative (if applicable)	Article 27
10	Data Breach Response and Notification Procedure	Articles 4, 33, 34
11	Data breach notification to Supervisory Authority (if applicable)	Article 33
12	Data breach notification to data subjects (if applicable)	Article 34

Some documentation is necessary only when specific *criteria* apply.

Conditionally mandated documentation	
Record of processing activities	If 250 employees or more, unless the processing is likely to result in a risk to the rights and freedoms of data subjects, is not occasional, or includes special categories of data or personal data relating to criminal convictions and offences
Consent form	If processing relies on consent as legal basis, and if the processing has been collected in written form[18]
Appointment of an EU representative	If processing involves subjects in the EU and is performed by a controller or processor not established in the EU, unless it is occasional, does not involve large scale processing, or special categories of data, or personal data relating to criminal convictions and offences, and is unlikely to result in risk to the rights and freedoms of natural persons
Data breach notification to Supervisory Authority	Only when a data breach that is likely to result in a risk to the rights and freedoms of natural persons occurs

[18] Indeed, the GDPR does not mandate the consent to be collected in written form. For more information, see European Data Protection Board, 'Guidelines 05/2020 on Consent', 16.

Data breach notification to data subjects	When a data breach that is likely to result in a high risk to the rights and freedoms of natural persons occurs or, when it is unlikely to result in a high risk, if the supervisory authority requires to do so

To make record keeping easier and consistent, the researcher should prepare appropriate templates for the steps to be documented or consult with the DPO or their legal department in lieu of the DPO, to check whether templates exist within the organization.

Before starting with the collection and processing of personal data, the researchers should collect data protection documentation already available in their organization, and create a specific *dossier* containing all the relevant documentation. New documents should be added to the *dossier* as soon as they are created. The purpose of the *dossier* is to record the steps and decisions taken by the researchers and other data protection stakeholders involved in the research activity and to present enough information to demonstrate that compliance has been maintained throughout the process.

The research team should look at the *dossier* not as a mere recording obligation. The *dossier* should act as the formalization of practical step that the research team takes to ensure the safeguards of the personal data. For instance, having a Data Breach Response and Notification Procedure is not sufficient. Researchers should be able to demonstrate that the procedure can be swiftly and effectively put into action, should necessity arise.

3.2.5 Verify if a Data Protection Impact Assessment is necessary

According to the Article 29 Working Party, a Data Protection Impact Assessment (DPIA) is "a process designed to describe the processing [of personal data], 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"[19].

Article 35.1 GDPR requires data controllers to perform a DPIA when the data processing is likely to result in a high risk to the rights and freedoms of natural persons. Therefore, a DPIA is not always mandatory. However, data controllers are required to always perform the preliminary risk assessment to identify whether the processing is likely to result in high risks to the rights and freedoms of natural persons. This preparatory assessment is an integral part of the DPIA process. Thus, it is possible to say that certain elements of the DPIA are mandatory to, at least, determine if a DPIA is necessary.

The risks to the rights and freedoms to data subjects are referred to in Recital 75 GDPR. These are the risks which could lead to physical, material, or non-material damage for the data subject concerned (e.g., being denied access to a service following a false-negative identification).

Examples of the risks to the rights and freedoms

[19] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679', October 2017, 4.

Discrimination	Identity theft or fraud
Financial loss	Damage to reputation
Loss of confidentiality of professional secrecy	Unauthorized reversal of pseudonymization
Economic or social disadvantage	Prevention from exercising control over personal data

The GDPR does not define 'high risk'. However, the Article 29 Working Party produced a list of nine *criteria* data controllers can follow to understand if the processing can be considered a high risk one[20].

***Criteria* for high-risk processing**	
Criterion 1	Evaluation or scoring (e.g., profiling)
Criterion 2	Automated decision-making with legal or similar significant effect
Criterion 3	Systematic monitoring
Criterion 4	Sensitive data or data of a highly personal nature
Criterion 5	Data processed on a large scale
Criterion 6	Matching or combining datasets (beyond reasonable expectations of data subject)
Criterion 7	Data concerning vulnerable data subjects
Criterion 8	Innovative use or applying new technological or organizational solutions
Criterion 9	When the processing in itself prevents data subjects from exercising a right or using a service or a contract

Researchers performing their research activities should consider all of them to understand whether a DPIA is required. Yet, *criteria* four and eight are particularly relevant for the purpose of this document. *Criterion* four matters when biometric data processed are processed during the research activity. *Criterion* eight is important in the context of ICT research since this activity might introduce new technology to process data (e.g., innovative ways to capture and analyze voice samples).

Article 35.4 GDPR requires national supervisory authorities to publish the list of data processing activities for which a DPIA is mandatory[21]. This might offer further

[20] Article 29 Data Protection Working Party, 9–11.

guidance as to what constitutes a processing required DPIA, and researchers should pay attention to the position of relevant supervisory authorities. Also, researchers should seek guidance from the organization's DPO, given the complexity of the task at hand.

In order to be able to demonstrate compliance, the assessment whether the processing is likely to result in high risks to the rights and freedoms of natural persons should be documented and kept.

3.2.6 Perform a DPIA (if necessary)

There is no standard way to perform a DPIA. However, Article 35.7 GDPR calls for specific elements that shall always be present. These are:

- a systematic description of the envisage processing operations;
- the purposes of the processing operations;
- an assessment of the necessity of the processing operations in relation to the purposes;
- an assessment of the proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- the technical and organizational measures envisaged to address the risks.

The researchers can include further elements to better describe the processing and the underlying risks. Also, if the data controller realizes, after having performed a DPIA, that the risks for the rights and freedoms of the data subject are not adequately mitigated by the measures envisaged to address such risks, the data controller shall seek prior consultation with the supervisory authority following the provision of Article 36 GDPR.

The law does not sanction a format for the DPIA. This can be freely chosen by the data controller. Some data protection authorities, however, have created templates data controllers can adopt[22].

The DPIA is not a point-in-time activity, but a continuous process. Thus, it might be necessary to perform multiple assessments over time, for instance when contextual elements change or when new information becomes available.

The results of DPIAs shall be recorded and stored as part of the data protection documentation.

3.2.7 Implement risk mitigating measures

According to Recital 78 GDPR "[t]he protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organizational measures be taken to ensure that the requirements of [the GDPR] are met". This provision, which represents a cornerstone of the legal framework, is further

[21] In this respect, national supervisory authorities have published in their websites the corresponding list. In some cases, the EDPB has already issued an opinion on the matter regarding the activities included in each list. For further information please see European Data Protection Board, 'Opinion 6/2019 on the Draft List of the Competent Supervisory Authority of Spain Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR)', March 2019.

[22] See for instance, Commision Nationale Informatique & Libertés, 'Privacy Impact Assessment (PIA). Templates', February 2018.

elaborated for the specific case of processing for research purposes. Recital 156 GDPR and Article 89 GDPR call for the implementation of 'appropriate safeguards', stressing the importance of safeguarding the rights and freedoms of natural persons.

The GDPR does not provide a comprehensive list of technical and organizational measures, leaving to the data controller the task of identifying them and assessing their effectiveness in mitigating risks for the data subjects. Also, researchers should consider external security and data protection audit, to confirm that the security and compliance measures are sound, and to further demonstrate compliance with the accountability principle.

Examples of technical and organizational measures	
Technical measures	**Organizational measures**
Data anonymization or pseudonymization[23]	Security policies
Encryption of communication	Data management plans
Protection of data from unauthorized access	Training program for personnel
Vulnerability assessment / Penetration testing	Regular audits and assessments

3.3 Execution phase

Once the research activity has been adequately prepared, the researchers can start their work and the related data processing operations. This stage begins with the collection of the data in accordance with the plan defined during the preparation phase.

3.3.1 Biometric data processing

Once the researchers have obtained the necessary biometric data, these can be processed to extract the biometric features to be employed in the research. Although it is theoretically possible to do it 'manually' (for instance, manually mapping the facial features in pictures, such as the distance between the eyes, the shape of the face, the height of the ears, etc.)[24], today such an approach is generally considered unfeasible and replaced with automated means often based on artificial intelligence technology (for specific guidance consult Part III on AI of these Guidelines). Regardless of this

[23] See also section 3.3.5 Erasure or destruction of data for more information on anonymization. For more technical information please refer to "Identification", "Pseudonymization" and "Anonymization" within Part II section "Main concepts" of these Guidelines)

[24] Some biometric recognition techniques have been first discovered as manual techniques, and even predates the birth of computing system. See for instance Mark Maguire, 'The Birth of Biometric Security', *Anthropology Today* 25, no. 2 (April 2009): 9–14, https://doi.org/10.1111/j.1467-8322.2009.00654.x..

distinction, any processing activity needs to be conducted adopting all the safeguards and precautions set during the preparation phase are respected.

3.3.2 Biometric system and user interface development

If the aim of the research is to develop a biometric system, the researchers should place particular care in the creation of the user interface, especially if the system will be used by the public. The interface should be designed as user-friendly as possible with the purpose of promoting transparency and facilitating data subjects to exercise their right to information. There are three main aspects researchers should consider: the information available through the user interface, the functionalities accessible through the user interface, and the general usability of the interface.

First, the data controller shall ensure that all the information provided to the data subjects following Articles 13 and 14 GDPR are available through the user interface. This should be easily accessible and presented in a clear and easy-to-understand way. For instance, the system might present a visible button the data subjects can click to open a pop-up window containing the information. It is advisable to have the information readily available in the system and avoid, if possible, links to external repositories or websites to minimize the risk of inaccessibility due to, for instance, connectivity issues. The user interface should also leverage on the capabilities of the device through which the information is accessed. For instance, in case the system runs on a smartphone, it could provide the option to call or send an email directly to the DPO with a simple click[25].

Second, the user interface should present a set of functionalities to make it easier for the data subjects to exercise their rights (provided that exemption for the application of such rights is not present. See section "Identify the data collection approach"). For instance, the user interface should make it possible for data subjects to access their personal data and rectify or delete them (insofar as this will not render the purpose of the processing impossible to achieve). Having specific functionalities accessible to data subjects will not only make it easier for them to exercise their rights but should also lower the burden on the data controllers, as many of these requests will be performed directly by the data subjects. For instance, users of facial recognition systems might need to update their pictures (e.g., after surgery). Giving them a direct way to do it, rather than having to contact the data controller, might incentivize them to keep the data updated and, therefore, will also ensure adherence to the principle of accuracy (see the "Accuracy" subsection in the Principles section of the General Part of these Guidelines). However, introducing these functionalities can also increase the risks to the rights and freedoms of the data subjects. For instance, in case the account of a user is violated, this 'self-service option' gives the attacker full control over the personal data of the data subjects. Therefore, the data controller shall always ensure that any additional risk introduced by specific functionalities is adequately mitigated by appropriate security measures (for instance, multi-factor authentication, mandatory password update, etc.). In case the researchers cannot adequately mitigate risks following the introduction of new functionalities, they shall seek prior consultation with relevant supervisory authority or avoid introducing the functionalities until they can find a feasible mitigation approach

[25] Notwithstanding, the contacts shall also be displayed, and the system shall not impose any specific means of communication.

(see the "Integrity and Confidentiality" subsection in the Principles section of the General Part of these Guidelines).

Third, the general usability of the interface shall promote transparency and avoid placing unnecessary burdens on the data subjects when exercising their rights. An adequate user interface should consider elements such as the characteristics of the data subjects (e.g., language, demographics, etc.), the way users interact with the system (e.g., on a PC, a smartphone, a custom hardware, etc.), the place where users interact with the system (e.g., at home, in a public space, etc.), fall-back options (e.g., when users accidentally change certain settings) and many other elements. Also, the developers should keep in mind that the system might be used by vulnerable subjects, such as children or visually impaired people. Therefore, the interface should be designed in a way to help them using the system (e.g., voice-to-text, text magnification, etc.).

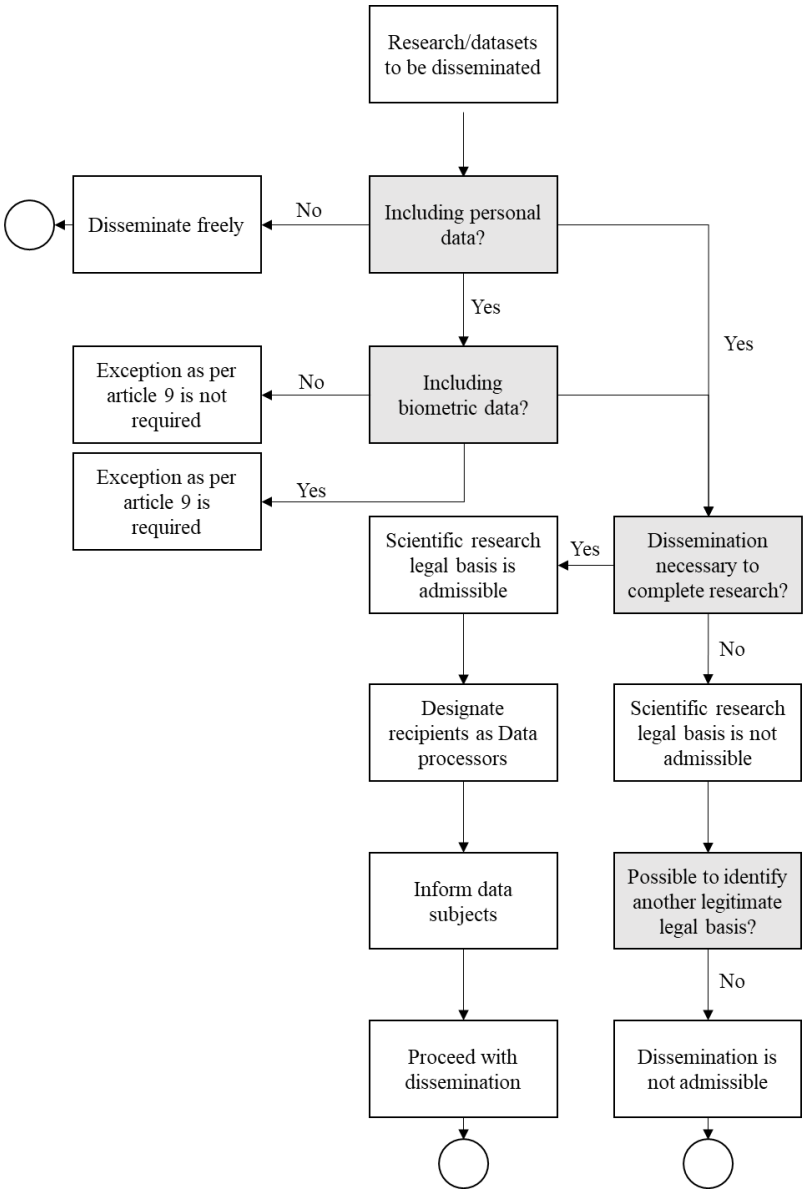
3.3.3 Biometric system testing

The final step before deploying the biometric system is to test it and validate its outputs. There are two possible scenarios. In the first one new data need to be collected, while in the second scenario the researchers employ the same data processed during the development phase. The first scenario occurs when, for instance, new subjects are brought in specifically for testing the system. In this case, the data controller needs to perform the steps already mentioned in regard to the preparation phase. In the second scenario, the researchers need to consider whether this further testing was comprised among the initial purposes (for more information see "Purpose limitation" in Part II, section "Principles"). Indeed, 'testing the system' configures a different processing than 'developing the system' and might therefore require a different legal basis, especially when the two processing require different sets of data. In such cases, the researchers should not assume that, since they complied with the obligations related to the development of the system, they automatically comply with those related to testing. It is important they look at this step with a critical approach and aim at minimizing risks to the rights and freedoms of the data subjects as their priority.

3.3.4 Dissemination of results

At the end of the research activity, the researchers might decide to disseminate their work. If the dissemination does not include the personal data processed during the research, the work can be disseminated to other interested parties. If the dissemination does include the data processed during the research (e.g., make the data available to the scientific community for peer review), then additional steps should be taken. The dissemination of personal data constitutes a processing operation as per Article 4.2 GDPR and – as described above – any processing operation involving biometric data shall be prohibited unless exemptions apply. Therefore, researchers should repeat the steps already described in 3.2.2 before proceeding with the dissemination. In particular, if the data controller relies on the 'scientific research' legal basis, and if all the requirements for adopting such legal basis are satisfied (see section 3.2.3 'Identify the most appropriate legal basis'), it is possible to further distinguish two scenarios. In the first one, the research team (Team A) has completed the research activity and intends to disseminate the data for the benefits of other research teams (Team B). In such a scenario, the dissemination is not a necessary operation for achieving the research purposes of Team A, but might be necessary for the research purposes of Team B.

Therefore, Team A cannot rely on the 'scientific research' legal basis. It follows that Team A does not have any legal ground to share the data with Team B, or any other recipient unless a different legal basis is found (for instance, Team A can collect explicit consent for the purpose of sharing data with Team B). In the second scenario, Team A realizes, after the collection of the personal data, that it does not have adequate capability (e.g., technical) to process the data and continue with the research. Therefore, Team A decides to rely on the capability of Team B to process the data. In this situation, the dissemination of data to Team B is a necessary step for achieving the research purposes of Team A, and Team B needs to be nominated as 'data processor' following the provisions of Article 28 GDPR. Article 4.8 GDPR defines a data processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". The designation and roles of the data processor shall be communicated to data subject prior to the transfer, and shall be governed by a contract or by Union or Member State law, which shall contain at least subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.



In case personal data need to be transfer outside the European Economic Area[26], and provided that such transfer is not subject to one or more of the derogations listed in Article 49 GDPR[27], additional steps should be taken. The GDPR envisages a number of instruments for international data transfer. However, not all of them are currently applicable, as relevant authority are still working to formalize some of them.

International data transfer	
Pursuing an adequacy decision	Applicable
Pursuing standard data protection clauses	Applicable

[26] Which includes all EU Member States and Iceland, Liechtenstein, and Norway.
[27] For more information, see also European Data Protection Board, 'Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679', May 2018.

Pursuing binding corporate rules	Applicable
Pursuing codes of conduct	Planned
Pursuing certification mechanisms	Planned
Pursuing legally binding instrument between public authorities or bodies	Planned[28]

In the first case (pursuing adequacy decision), the data can be transferred to extra EU states if there is an adequacy decision by the European Commission. An adequacy decision can be adopted if the other state offers a level of data protection adequate to the European Standard[29]. In the second case, (pursuing standard data protection clauses), the data can be transferred if there is an agreement between the data exporter and the data importer and if such agreements contain a number of standard clauses regarding data protection that have been pre-approved by the European Commission[30]. In the third case, if the extra-territorial transfer is occurring within the same entity (e.g., a transfer between two branches of an international group), the data can be transferred if there are corporate binding rules that offer data protection safeguards as per Article 47 of the GDPR and are approved by competent data protection supervisory authority.

3.3.5 Erasure or destruction of data

At the end of the testing, the controller should delete the dataset used for this purpose, unless there is a lawful need to maintain them, for instance for the purpose of refining or evaluating the system, or for other purposes compatible with those for which they were collected in accordance with the conditions set by Article 9.2 GDPR.

See: "Identification", "Pseudonymization" and "Anonymization" within Part II section "Main concepts" of these Guidelines)

[28] As of July 2021, these three options for international data transfer have been planned but not implemented yet.

[29] The list of countries recognized through an adequacy decision can be accessed at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[30] The most up-to-date version of the standard clauses can be found in European Commission, 'Implementing Decision 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council' (2021), https://doi.org/10.5040/9781782258674.

4 Biometric technology in ICT research and innovation. Case study

The following section presents an application of the contents of section 3 'Biometric technology in ICT research and innovation. Guidelines'. The case study does not refer to any real situation.

A team of ICT developers decides to design a hand-recognition system to streamline the identification process of employees at the entrance of work sites. The aim of the researchers is to propose a privacy preserving approach, understanding its feasibility, develop the corresponding technology, and publish a paper with the results.

The team of developers decides to put emphasis on three aspects:

- The system fully complies with data protection norms
- The system is effective enough to be adopted by organizations
- The system is not perceived by users – employees – as too invasive

All the developers work for the same private company, Developing Inc. This is based in the fictional European State of Developonia. In the scenario, Developing Inc. acts as data controller.

4.1 Design phase

4.1.1 Identify the goals and whether the activity qualifies as 'research'

The developers establish the following goals:

- to design an approach to streamline the identification of employees at work sites
- to understand its feasibility
- to develop and test the corresponding technology
- to publish a paper with the results.

Informed by the goals, the developers proceed to assess if the project is a 'scientific research'. To do so, they consider the definition from the EDPS (see section 2.5 "Research activity") and assess if the activity helps "growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests"[31]. The developers conclude the answer is positive, since the activity does not aim to merely create a new commercial technology, but to introduce a privacy preserving approach for workers that will be informative for privacy preserving applications in other contexts.

Legal regime: research			
Does the activity qualify as 'research'?	Yes	?	Specific regime on research applies
	No		Specific regime on research does not apply

[31] European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research'.

4.1.2 Confirm the need to process biometric data

For the specific research, the developers decide not to rely on a commercial database, nor to use computer-generated images. The developers decide to collect all the data (palmprints) that are necessary to achieve the goals of their research directly from natural persons. The developers will collect impressions of the palmprints and extract the distinctive physical features (e.g., measurements of the hand) from these impressions.

To understand if biometric data are involved, developers adopt the *criteria* of article 4.14 GDPR.

Biometric data checklist		
☒	Amount to personal data	Yes, since palmprints relate to an 'identified natural person'
☒	Are based on specific technical processing	Yes, since the distinctive features will be extracted from palmprint impressions using technical processing
☒	Pertain to physical, physiological or behavioral characteristics	Yes, since palmprints relate to physical characteristics
☒	They allow or confirm unique identification of natural persons	Yes, since the goal of the project is to use palmprints to identify natural persons

Legal regime: special categories of personal data			
Does the activity involve biometric data	Yes	☒	Specific regime on special categories of personal data applies
	No		Specific regime on special categories of personal data does not apply

4.2 Preparation phase

4.2.1 Appoint a Data Protection Officer (DPO)

To assess the need for a DPO, the developers look at the requirements in article 37 GDPR. Since these often mention the 'large scale' *criterion*, the developers decide to first assess if the processing can be considered of large scale, adopting the Article 29 Working Party approach.

Assessment for the 'large scale' criterion	
Number of data subjects concerned	30 to 50 data subjects expected
Volume of data and/or range of different data items being processed	Personal data (e.g., name, age, etc.) and special categories of data (palmprints) will be processed
Duration or permanence of the data processing activity	The developers expect the study to last a year
Geographical extent of the processing activity	The developers expect the study to have local extent (municipality)

After the assessment, the developers decide the processing activity can be configured as a 'large scale' one. Even if quantitative *criteria* are not available and, therefore, the result of the assessment cannot be considered conclusive, they decide as such with a view on maintaining a more cautious approach.

After having assessed the 'large scale' *criterion*, the developers proceed to assess the need for a DPO.

Requirements mandating a Data Protection Officer		
"The processing is carried out by a public authority or body, except for courts acting in their judicial capacity"	?	Does not apply
"The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale"	✗	Does not apply (no regular nor systematic monitoring)
"The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9"	✓	Applies (special categories of data and 'large scale' processing)

"The core activities of the controller or the processor consist of processing on a large scale of […] personal data relating to criminal convictions and offences referred to in Article 10"	✗	Does not apply (no personal data related to criminal convictions and offences)
In every other case not listed by requirements 1-3, "the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer"	?	Does not apply (no specific EU or MS law)

Since one of the requirements applies, the developers decide to designate a DPO. The data controller (Developing Inc.) does not have an appointed DPO. Therefore, the developers proceed to hire one.

Legal regime: special categories of personal data			
Does the activity satisfy one of the requirements for a DPO	Yes	?	Designation of a DPO is mandatory
	No		Designation of a DPO is optional

4.2.2 Identify the data collection approach

The developers decide to collect personal data directly from the data subjects. They will be invited to the laboratory of Design Inc., where impressions of the palmprints will be taken.

4.2.3 Identify the most appropriate legal basis

Before identifying the most appropriate legal basis, the developers need to assess if one of the exemptions to the processing of special categories of personal data applies.

Available legal bases provided by the GDPR to process biometric data		
Explicit consent	?	Applies
Employment, social security, and social protection	?	Does not apply (requires additional law; a compliance assessment confirmed it does not exist in the State)
Vital interests	?	Does not apply
Activities from associations and other not-for-profit	?	Does not apply

entities		
Data have been published by the data subject	?	Does not apply
Legal claims or judicial acts	?	Does not apply
Substantial public interest	?	Does not apply (requires additional law; a compliance assessment confirmed it does not exist in the State)
Health or social care	?	Does not apply (requires additional law; a compliance assessment confirmed it does not exist in the State)
Health public interest	?	Does not apply (requires additional law; a compliance assessment confirmed it does not exist in the State)
Archiving, research, and statistics	?	Does not apply (requires additional law; a compliance assessment confirmed it does not exist in the State)

Since the only applicable exemption is 'explicit consent', the developers also decide to adopt 'consent' as legal basis for data processing.

Having regarded the legal basis and considering that the collection will occur directly from the data subjects (see section 4.2.2 'Identify the data collection approach'), the developers prepare the information that will be provided to the data subjects in the consent form.

Information to be provided to data subjects according to the collection approach	
The identity and contact details of the controller	Developing Inc. (data controller) Developers Street, 99, 21010, Developonia +00 – 0123456, info@developinginc.com
If applicable, the identity and contact details of the controller's representative	Not applicable
The contact details of the data protection officer	John Doe (DPO of Developing Inc.) Developers Street, 99, 21010 Developonia +00 – 0123457, dpo@developinginc.com
The purposes of the processing	Research an approach to use palmprints to identify workers at work sites, develop and test its technology, and publish the results
The categories of personal data concerned	Name, surname, birthdate, address, phone number, email, palmprint impressions
The legal basis for the processing	Explicit consent
If applicable, the legitimate interests pursued by the controller or by a third party	Not applicable (no legitimate interest pursued)
Recipients or categories of recipients of the personal data	Developing Inc. (data controller)
The intention of the controller to transfer personal data to a third country or international organization	Not applicable (no transfer)
In case of transfer, the existence or absence of an adequacy decision, or reference to the safeguards and the means by which to obtain a copy of the data	Not applicable (no transfer)
The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period	Duration of the research (expected to start on 0101/2022 and last a year), until the system is developed and tested
The existence of the right to access, rectification or erasure, restriction of	Data subjects can exercise their rights as per articles 12-22 GDPR

processing, objection, and portability	
In case of 'explicit consent' as legal basis, the existence of the right to withdraw consent at any time and without any negative consequence	Data subjects can withdraw consent. If this occurs, Developing Inc. will identify new data subjects
The right to lodge a complaint with a supervisory authority	Complaints can be lodged with the DPA of Developonia. Contacts will be provided
Whether the provision of data is a statutory or contractual requirement, or necessary to enter into a contract, if the data subject is obliged to provide the data and the consequences of failure to provide	The provision is not a statutory or contractual requirement
The existence of automated decision-making, including profiling	The processing does not include automated decision-making
In the case of automated decision-making, information on the logic involved, its significance and the envisaged consequences for the subject	Not applicable

4.2.4 Create a repository for supporting documentation

The DPO of Developing Inc. creates a repository where the documentation concerning the processing is archived. The documents are stored locally in the servers of Developing Inc. The storage architecture of Developing Inc. is redundant to ensure business continuity, and the contents of the servers are periodically backed up.

The developers identify the following mandatory documentation:

Documentation: checklist		
Personal data protection policy	?	Applies
Privacy notice	?	Applies
Data retention policy	✓	Applies
Data retention schedule	✓	Applies
Record of processing activities (if applicable)	?	Applies (see below)

Consent form (if applicable)	?	Applies (consent as legal basis)
Data processing agreement with suppliers	?	Does not apply (no suppliers with access to personal data)
Data Protection Impact Assessment	✓	Applies (see section 4.2.5)
Contractual clauses for the transfer of personal data (if applicable)	?	Does not apply (no transfer)
Appointment of an EU representative (if applicable)	?	Does not apply (Developing Inc. is based in the European Union)
Data Breach Response and Notification Procedure	✓	Applies
Data breach register	?	Does not apply (no breach has occurred)
Data breach notification form to the Supervisory Authority	✗	Does not apply (no breach has occurred)
Data breach notification form to data subjects	?	Does not apply (no breach has occurred)

In the scenario, Design Inc. does have a record of processing activities. Indeed, even though it is a small organization with less than 250 employees, it performs data processing on its employees on a regular basis (e.g., managing salary, organizing corporate retreats, etc.). Developing Inc. has not produced a proprietary template for the record of processing activities and has adopted the one provided by the French Supervisory Authority[32].

4.2.5 Verify if Data Protection Impact Assessment is necessary

The GDPR requires a DPIA when the data processing is likely to result in a high risk to the rights and freedoms of natural persons. The developers, unsure if the processing poses such risks, decide to assess the processing adopting the aforementioned nine *criteria* suggested by the Article 29 Working Party.

***Criteria* for high-risk processing**		
Evaluation or scoring (e.g., profiling)	?	Does not apply
Automated decision-making with legal or similar significant effect	?	Does not apply

[32] The template can be accessed at Commision Nationale Informatique & Libertés, 'Record of Processing Activities', August 2019, https://www.cnil.fr/en/record-processing-activities.

Systematic monitoring	☐	Does not apply
Sensitive data or data of a highly personal nature	☐	Applies (see below)
Data processed on a large scale	☐	Applies (see section 4.2.1)
Matching or combining datasets (beyond reasonable expectations of data subject)	☐	Does not apply
Data concerning vulnerable data subjects	☐	Does not apply
Innovative use or applying new technological or organizational solutions	✗	Does not apply (see below)
When the processing in itself prevents data subjects from exercising a right or using a service or a contract	☐	Does not apply

The assessment reveals that the processing satisfies at least two *criteria*. The first one regards the type of personal data that are going to be processed. Since, in the context of this research activity, palmprints have been established as biometric data, the developers conclude that these data satisfy the *criterion* of being sensitive and of a highly personal nature. The second *criterion* regards the scale of the processing. The developers already established that the processing qualifies as a 'large scale' one (see 4.2.1 "Appoint a Data Protection Officer (DPO)").

The developers interrogate themselves also on the 'Innovative use or applying new technological or organizational solutions' *criterion*. It does not apply since the activity is focused on research and concrete application to an organizational context is not envisioned in the current activity.

Data Protection Impact Assessment			
Is the processing a 'high risk' one	Yes	☐	DPIA is mandatory
	No		DPIA is optional

4.2.6 Perform a DPIA

Given that Developonia supervisory authority hasn't drafted guidance on how to conduct a DPIA, and following the advice of the DPO, the developers perform the DPIA using the guidance from the Article 29 Working Party, as endorsed by the EDPB, and the template provided by the French Supervisory Authority[33]. The result of the

[33] Commision Nationale Informatique & Libertés, 'Privacy Impact Assessment (PIA). Templates'.

DPIA shows that all the risks for the rights and freedoms of data subjects are mitigated to an acceptable level, which is never high for all the identified risks.

The result of the DPIA is stored in the repository for supporting documentation.

4.2.7 Implement risk mitigation measures

After performing the DPIA, the developers establish that the technical and security measures are appropriate to protect the rights and freedoms of data subject and can be considered appropriate safeguards as per article 89 GDPR.

4.3 Execution phase

4.3.1 Biometric data processing

The team of researchers, after having distributed all the information to the data subjects and having collected their explicit consent, proceed to collect the biometric data of subjects. The researchers take impressions of the hands of each participant and feed these to an artificial intelligence system to extract the biometric features (e.g., hand shapes, ridges and valleys, etc.). All the components of the artificial intelligence system, including the underlying algorithm are developed and maintained in-house by the researchers, and no other subjects are involved or access the data processed by the artificial intelligence system. The artificial intelligence components of the system are developed following the steps detailed in Part III of this document.

4.3.2 Biometric system user interface development

The research team decides that the interaction with the biometric system will happen through dedicated kiosks. During the research, the kiosks will be placed in the laboratory of the developers. The kiosks will collect data and store them locally, and users will interact with the kiosks in the presence of the research team. The use of the kiosks in the controlled environment of the laboratory will inform the developers of the feasibility of the technology and will act as a pilot test for future deployment on actual working sites.

One of the goals of the research is to streamline the authentication of workers. To achieve such goals, researchers aim to make the authentication process quicker by increasing the ease of use, thus minimizing the time spent by each user at the kiosk. For this reason, they decide to split the functionalities into two different kinds of kiosk: one dedicated to authentication (authentication kiosk), and one dedicated to other functionalities, such as accessing information and updating personal data (extra kiosk). This way workers who need to perform actions other than authentication will not slow down the authentication of other workers.

The authentication kiosk has two main components: a scanner for the hand and a monitor. If the authentication is successful, a green mark is displayed, the door opens, and the worker can proceed. The authentication is not recorded (since the goal is not to measure the working hours of individuals), and the monitor does not display any information on the person.

The extra kiosk has the same elements of the authentication kiosk, with the difference that the monitor is touchscreen to ensure users can interact with the system. Also, the extra kiosk is boxed to avoid shoulder surfing. Users can activate the extra kiosk by simply scanning their hands. When this is done, the monitor displays a menu with three options:

- Display data processing information: this option opens a pop-up window where all the information listed in section 4.2.3 "Identify the most appropriate legal basis" are provided;
- Access and rectify personal data: this option opens a pop-up window where all the personal data of the subjects are displayed, and where the user can rectify such data, including recording new palm impressions;
- Exercise right to rectification, restriction, data portability or objection: this option is currently disabled in the research prototype kiosk. If a user selects it, members of the research team receive an alert on their mobile devices and are required to verify with the data subjects whether they intend to exercise any of their rights.

4.3.3 Biometric system testing

Once the system has been developed, researchers can test it and verify its performance (e.g., error rate, speed of authentication, energy consumption, etc.). To do so, they gather the data subjects to simulate the use of the system.

Since testing the system is one of the key activities of the research, the data subjects have already provided explicit consent to the testing, and no additional personal data are processed, the research team concludes that the risks for the rights and freedoms of the data subjects are adequately addressed and proceed with the testing.

4.3.4 Dissemination of results

Once the testing activity has been completed, and all the testing data have been gathered, the research team can finally draft a paper where the technology is described, and the outcomes are presented. Confident that the system will perform consistently, they decide to make the technology open-source to ensure that other researchers can perform their own testing and validate the results. Following this decision, the researchers decide to delete all the personal data of the subjects who took place in the research activity.

4.3.5 Erasure or destruction of data

All the personal data are deleted completely.

These checklists have not been revised and validated externally. Nonetheless, PANELFIT strongly considers them as adequate for the purpose that these Guidelines are aimed at.

Design phase checklist

Step	Guidelines' relevant section
☐ Identify the goal(s) of the activity	3.1.1
☐ Assess if the activity amounts to 'research'	3.1.1
☐ Identify the roles of the research team and other stakeholders	3.1.1
☐ Confirm that processing biometric data is necessary to reach the goal(s) of the activity	3.1.2

Preparation phase checklist

Step	Guidelines' relevant section
☐ Assess if one of the five requirements for a DPO apply	3.2.1
☐ If public authority, check if DPO can be nominated by another public authority	3.2.1
☐ Publish the contact of the DPO	3.2.1
☐ Identify if data collection will occur directly from the data subjects or indirectly	3.2.2
☐ Assess if you are eligible for an exemption from the obligation to inform the data subject	3.2.2
☐ Record the assessment of the eligibility for an exemption from the obligation to inform	3.2.2
☐ Define an internal process to ensure the accuracy of the data processed	3.2.2
☐ Identify if exemptions to the processing of special categories of personal data apply	3.2.3
☐ If additional law is required, verify its existence. If none, identify another exemption	3.2.3

☐ If exemptions apply, identify the legal basis for the data processing as per Article 6 GDPR	3.2.3
☐ If rely on consent, make sure it is explicit	3.2.3
☐ Keep a record of consent forms	3.2.3 / 3.2.4
☐ Create a repository of documents, which contains at least the documents mandated by GDPR	3.2.4
☐ Assess if the processing introduces high risk to the rights and freedoms of natural persons	3.2.5
☐ Record the results of the preliminary assessment	3.2.5
☐ If the processing introduces high risks, perform a DPIA	3.2.6
☐ If risks are not mitigated by the envisaged measures, implement additional adequate measures	3.2.7
☐ If risks are not mitigated and it is not possible to implement additional measures, consult with supervisory authority	3.2.7
☐ Record the results of the DPIA	3.2.4 / 3.2.6 / 3.2.7

Execution phase checklist

Step	**Guidelines' relevant section**
☐ Process data applying safeguards and precautions set during the Preparation phase	3.3.1
☐ In case of ICT system development, ensure the data subject can access necessary information through appropriate user interface	3.3.2
☐ In case of ICT system development, assess the risks for the data subjects related to every function of the system	3.3.2
☐ Record the result of the assessment of risks related to system functions	3.2.4 / 3.3.2
☐ If risks cannot be mitigated, consult with supervisory authority or do not implement	3.3.2
☐ Keep in mind use cases involving vulnerable subjects	3.3.2
☐ In case of ICT system testing, assess if testing the system configures a different processing from developing the system	3.3.3

☐ Record the result of the assessment about testing as a different processing	3.2.4 / 3.3.3
☐ If testing the system configures a different processing, assess if purpose is compatible	3.3.3
☐ Record the result of the compatibility test	3.2.4 / 3.3.3
☐ Assess if dissemination of the outcome involves disseminating personal data and special categories of personal data as well	3.3.4
☐ Identify exemptions to processing special categories of personal data prior the dissemination	3.3.4
☐ Identify the most appropriate legal basis to process personal data prior to the dissemination	3.3.4
☐ Designate recipients as Data processors	3.3.4
☐ Inform data subjects of the data transfer	3.3.4
☐ Check if data transfer is international	3.3.4
☐ If transfer is international, and no derogations apply, identify an instrument for transfer	3.3.4
☐ Assess if lawful to retain personal data	3.3.5
☐ Record the result of the assessment on the lawfulness of data retention	3.2.4 / 3.3.5
☐ If unlawful to retain personal data, delete or anonymize them	3.3.5