



PROCESSING OF BIOMETRIC AND GENETIC DATA

European Standards



TBILISI
2022

AUTHORS OF THE STUDY:

KETEVAN KUKAVA

Rule of Law and Human
Rights Direction Head, IDFI

SALOME CHKHAIDZE

Lawyer/Researcher,
IDFI

NATA AKHALADZE

Lawyer,
IDFI



Kingdom of the Netherlands



Institute for Development
of Freedom of Information



**STATE
INSPECTOR'S
SERVICE**

The study was prepared within the framework of the project “Promoting Personal Data Protection in Georgia” funded by the Embassy of the Netherlands in Georgia. Opinions expressed in this document do not necessarily reflect the position of the Embassy of the Netherlands.

ISBN 978-9941-8-4136-1

PROCESSING OF BIOMETRIC AND GENETIC DATA

European Standards

**TBILISI
2022**

CONTENTS

1. INTRODUCTION	6
2. PROCESSING OF BIOMETRIC DATA	9
2.1. THE CONCEPT OF BIOMETRIC DATA	10
2.2. AREA OF APPLICATION OF BIOMETRIC DATA	12
2.3. RISKS AND THREATS RELATED TO BIOMETRIC DATA PROCESSING	14
2.4. STANDARDS OF BIOMETRIC DATA PROCESSING	15
2.4.1. The principle of lawfulness, fairness and transparency of processing	16
2.4.2. Purpose limitation principle	17
2.4.3. The principle of data minimisation	18
2.4.4. The principle of data accuracy	18
2.4.5. Limiting the storage period of biometric data	19
2.4.6. Ensuring the security of biometric data	19
2.4.7. The principle of accountability	22
2.5. PROCESSING OF DATA IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY	22
3. PROCESSING OF GENETIC DATA	24
3.1. THE CONCEPT OF GENETIC DATA	25
3.2. AREA OF THE USE OF GENETIC DATA, RISKS AND THREATS ASSOCIATED WITH THEIR PROCESSING	27
3.3. THE PRINCIPLE OF PROHIBITION OF DISCRIMINATION AND STIGMATIZATION ON GENETIC GROUNDS	29
3.4. SCOPE, PRINCIPLES AND GROUNDS FOR GENETIC DATA PROCESSING	31
3.4.1. Principles of genetic data processing	31
3.4.2. Grounds for genetic data processing	35
3.4.2.1. <i>Consent of the data subject</i>	36
3.5. THE RIGHT TO RECEIVE AND REFUSE TO RECEIVE INFORMATION	37

4. JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS	39
4.1. S. AND MARPER V. THE UNITED KINGDOM	40
4.2. M.K. V. FRANCE (2013)	42
4.3. GAUGHRAN V. THE UNITED KINGDOM (2020)	43
4.4. P.G. AND J.H. V. THE UNITED KINGDOM (2001)	44
4.5. AYCAGUER V. FRANCE (2017)	46
5. JUDGMENTS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION	48
5.1. MICHAEL SCHWARZ V STADT BOCHUM (2013)	49
5.2. W. P. WILLEMS AND OTHERS V BURGEMEESTER VAN NUTH AND OTHERS (2015)	50
6. SUMMARY	52



1. INTRODUCTION

Data related to a person's physical, biological, or physiological characteristics that enable an individual to be uniquely identified is considered to be biometric data.¹ Using this kind of data can help to raise the security level and make identification and authentication procedures easy, fast and convenient. Technological progress has made biometric systems more accessible, but with the consequent positive results, new threats have emerged.²

Data protection authorities, civil liberties groups and some scholars have followed the growth of biometric technologies with a critical eye. A point of departure for their concern is the automation of biometric identification and authentication schemes.³ In the words of the WP29,⁴ these schemes change irrevocably the relation between body and identity, because they make the characteristics of the human body "machine-readable" and subject to further use.⁵

Besides, in recent years the extraction of many types of personal data from human biological material has reached enormous scales, in which genome sequencing has played a special role. The accuracy and scope of genetic testing within and beyond studies and treatments have increased, and the increase in scale has been facilitated by a drastic reduction in the cost of genome sequencing.⁶

Advances in genetic data processing technologies help researchers better study different diseases, identify ways to prevent and treat them, and acquire vital importance to humans and their health. Each person's genetic makeup is common to him/her, his/her family members, and the group to which he/she belongs. Consequently, genetic testing in order to assess health risks or to determine biological relationships affects not only the right to privacy of an individual but also raises the issue of privacy of a group of individuals. The indelible nature of genetic information and its potential implications for discriminatory treatment make it particularly sensitive.⁷

The growing ability to obtain a wide variety of information about humans as a result of genetic data processing and the unique nature of DNA makes it essential to exercise proper control over them and to have effective mechanisms for protecting privacy.

With the adoption of the General Data Protection Regulation (GDPR),⁸ the Data Protection Directive

¹ 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, Par. 58, available at: <https://bit.ly/3kF2S6l> Date of access: 21.07.2021.

² Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

³ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, p. 209.

⁴ Advisory body that was based on the Data Protection Directive.

⁵ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, p. 209.

⁶ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation, A Commentary, Oxford University Press, 2020, p. 197.

⁷ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, p. 85.

⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, available at: <https://bit.ly/3C6j2Le> Date of access: 20.07.2021.

2016/680 for the police and criminal justice authorities,⁹ as well as with the modernization of Council of Europe Convention 108,¹⁰ legal instruments have emerged to regulate the processing of biometric and genetic data across Europe.

The General Data Protection Regulation, considered to be the most complex legal framework for data protection in the world, does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences.¹¹ Such processing is regulated by Directive 2016/680. Herein, neither the General Data Protection Regulation nor Directive 2016/680 applies¹² to the collection, storage, processing and exchange of data for national security purposes. The EU has no direct legislative power in this area, as under the Treaty on European Union, national security remains the sole responsibility of each Member State.¹³

As for the Modernised Convention 108, it considers inadmissible a complete exception to the processing of data for the purposes of national security and defense. Exceptions are allowed only in respect of certain provisions, on the condition that such exceptions are provided for by law, that they respect the essence of the fundamental rights and freedoms, and are necessary in a democratic society.¹⁴ Notwithstanding the exceptions allowed, the requirement that processing activities for national security and defense purposes be subject to an independent and effective review and supervision is laid down in the convention.¹⁵

The present study reviews the concept and area of application of biometric and genetic data, the threats and risks associated with their processing, and analyzes the principles and grounds for processing such data. The study also discusses certain judgments delivered by the European Court of Human Rights and the Court of Justice of the European Union regarding the processing of biometric and genetic data.

⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data available at: <https://bit.ly/3kTaS3d> Date of access: 20.07.2021.

¹⁰ Available at: <https://bit.ly/3qqm0lp> Date of access: 20.07.2021.

¹¹ General Data Protection Regulation, article 2 (2)(d).

¹² General Data Protection Regulation, article 2 (2); 2016/680 Directive, article 2.

¹³ Treaty on European Union, Article 4(2), available at: <https://bit.ly/3cd5mDw> Date of access :14.11.2021.

¹⁴ 108+ convention, article 11.

¹⁵ The Modernised Convention 108: novelties in a nutshell, available at: <https://bit.ly/3caNkBX> Date of access: 14.11. 2021.



2. PROCESSING OF BIOMETRIC DATA

2.1. THE CONCEPT OF BIOMETRIC DATA

According to Modernised Convention 108, biometric data is related to physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual.¹⁶ Examples of such biometric data are provided by fingerprints, retinal patterns, facial structure, voices, but also hand geometry or even some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystrokes, a particular way to walk or to speak, etc.).¹⁷ Indeed, because of their unique link to a specific individual, biometric data may be used to identify the individual.¹⁸

The EU General Data Protection Regulation gives biometric data, the purpose of which is the unique identification of an individual, the status of a special category of data.¹⁹ Similar to the mentioned regulation, an expanded list of special categories of data is provided by the Modernised Convention 108²⁰ and Directive 2016/680,²¹ and they include biometric data by which a person is identified.

Biometrics may be divided in various ways, one of them being “strong”, “weak”, and “soft” identifiers. Strong identifiers allow or confirm the unique identification of a natural person, e.g. fingerprints, iris, and retina. Weak biometrics are features that are “less unique” or “less stable”, e.g. body shape, behavioural patterns, voice, etc. Soft biometrics comprises features that are generic in nature and not uniquely associated with a person, e.g. gender or age.²² However, requiring uniqueness by the GDPR can be silencing towards soft biometric traits.²³

According to the GDPR, “biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.²⁴

Article 4(14) of the GDPR does not define the processes of generating or applying biometrics. It relates to the data resulting from specific technical processing but its explication of these processes

¹⁶ 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, par. 58, available at: <https://bit.ly/3kF2S6l> Date of access: 21.07.2021.

¹⁷ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, available at: <https://bit.ly/3kET3W4> Date of access: 21.07.2021.

¹⁸ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, available at: <https://bit.ly/3kET3W4> Date of access: 21.07.2021.

¹⁹ General Data Protection Regulation, article 9, available at: <https://bit.ly/3Bn9Vqh> Date of access: 21.07.2021.

²⁰ 108+ convention, article 6(1).

²¹ 2016/680 Directive, article 10.




²² Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, p. 13, available at: <https://bit.ly/30QyFKd> Date of access: 24.12.2021.

²³ Tamas Bisztray, Nils Gruschka, Thirimachos Bourlai, Lothar Fritsch, Emerging biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks, 2021, available at: <https://bit.ly/3yTCKcY> Date of access: 24.12.2021.

²⁴ General Data Protection Regulation, article 4(14).

is vague as it does not specify what specific technical processing is.²⁵ For instance, according to Article 4(13) of the GDPR DNA is included in the definition of genetic data and it may as well constitute a biometric reference measure (within the scope of specific technical processing) and according to Article 4 (15), it also is regarded as data concerning health. These overlaps, however, do not appear to create difficulties in applying the GDPR. In this regard, it bears emphasis that Article 9(4) of the GDPR accords Member States considerable leeway in how they regulate the processing of genetic data, biometric data and data concerning health.²⁶

In accordance with Articles 4 (14) and 9 of the General Data Protection Regulation, the definition of biometric data includes the following three components:

-  Nature of data: data relating to physical, physiological or behavioural characteristics of a natural person;
-  Means and way of processing: data “resulting from a specific technical processing”;
-  Purpose of processing: data must be used for the purpose of uniquely identifying a natural person.²⁷

Video footage/photograph is included in the concept of biometric data when it is processed using specific technical means and the individual is uniquely identified or authenticated.²⁸ The definition of biometric data in the General Data Protection Regulation and Directive 2016/680²⁹ requires a “specific technical processing” component. Consequently, video footage, photographs or audio recordings taken separately may not be regarded as biometric data under Article 9 of the GDPR and may not be subject to stronger protection guarantees. According to the definition, it is the nature of the processing that is crucial for the data to be considered biometric.³⁰

²⁵ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR), A Commentary*, Oxford University Press, 2020, p. 212.

²⁶ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR), A Commentary*, Oxford University Press, 2020, p. 213.

²⁷ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. par. 76, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

²⁸ General Data Protection Regulation, recital 51; Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020. Par. 74, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

²⁹ 2016/680 Directive, article 3(13).

³⁰ Els Kindt, *A First Attempt at Regulating Biometric Data in the European Union*, 2020, available at: <https://bit.ly/3iNntmH> Date of access: 21.07.2021.

2.2. AREA OF APPLICATION OF BIOMETRIC DATA

Biometric systems identify people or verify their identities based on the automated comparison of the human characteristic(s) (using data stored in databases).³¹ However, it is important to note that beyond identification, biometric data can provide detailed information about people (e.g., health conditions), as biometric technology sensors rely on the human body's characteristics.³²

Biometrics, usually in combination with AI systems, also play a role in modern diagnostic techniques. For instance, in the UK, an AI tool was developed that can identify signs of eye disease by scanning the patient's retina.³³

Because of the considerable potential of the automated use of biometric characteristics and the promises of secure methods of identification and identity or other claim verification, biometric systems have been widely introduced in the public and the private sector.³⁴ Biometric technologies have been used for a long time mainly by governmental authorities, but recently the situation has gradually shifted to one where commercial organisations play a primary role using these technologies and developing new products.³⁵ One of the key drivers of that change is that the technology has matured. In that sense, biometrics are replacing or enhancing conventional identification methods, particularly those based on multiple identification factors needed for strong authentication systems.³⁶

In the public sector, biometric systems are used by public authorities as a method for the verification of the authenticity of documents and the identity of the holder (for example, of identity documents).³⁷ At the same time, law enforcement authorities start to use more extensively automated fingerprinting systems often in cooperation with law enforcement authorities in other countries. As for the private sector, the deployment of biometric systems varies from the use for increasing the security of access control to places, networks and information, to the use for administrative purposes and convenience reasons.³⁸

In addition, fingerprint and face recognition software are often built into modern smartphones, tablets/tablets and laptops.³⁹ Some companies also use face recognition technology to control the work-

³¹ Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, 2013, p. 19.

³² Digital identity and biometrics: When your face reveals your vaccination status ... and more, available at: <https://bit.ly/3yQM5Cj> Date of access: 22.12.2021.

³³ Ch. Wendehorst, Y. Duller, *Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, 2021, p.18, available at: <https://bit.ly/30QyFKd> Date of access: 22.12.2021.

³⁴ Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, 2013, p. 64.

³⁵ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

³⁶ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

³⁷ Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, 2013, p. 64.

³⁸ Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, 2013, p. 65.

³⁹ National Cyber Security Centre of UK, *Using Biometrics*, available at: <https://bit.ly/3msYfMP> Date of access: 22.12.2021.

ing hours of their employees.⁴⁰

Unlike a password or certificate, biometric data collected during an authentication or identification procedure reveals more information about the person.⁴¹ Depending on the biometric data collected, data can be derived from the subject such as race or gender (even from fingerprints), emotional state, diseases, genetic characteristics and tares, substance consumption, etc. Since this information is “built-in”, the user cannot prevent the collection of such additional information.⁴²

Biometric **identification** of an individual involves the process of comparing biometric data of an individual to several biometric templates stored in a database, while **the individual verification/authentication process** includes comparing the biometric data of an individual to a single biometric template stored in a device.

As a result of technological development, it is possible to use biometric systems for **categorization/segregation** purposes. This means determining whether a person’s biometric data belongs to a predetermined group, such as people of a certain age or gender. In this case, the identification and verification of the individual are not important, because as a result of this process he/she automatically belongs to a specific category of people. For example, people may see different ads based on their age or gender. When the purpose of data processing is to distinguish one group of people from another but not to uniquely identify an individual, such processing does not fall within the scope of Article 9 of the GDPR.

Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates to uniquely identify persons but instead just detects those physical characteristics to classify the person then the processing would not fall under Article 9 (as long as no other types of special categories of data are being processed).⁴³

If a controller wishes to detect a data subject re-entering the area or entering another area (for example in order to project continued customized advertisement), the purpose would then be to uniquely identify a natural person, meaning that the operation would from the start fall under Article 9 of the GDPR.⁴⁴

If a shop owner has installed a facial recognition system inside his shop to customize its advertisement towards individuals, the data controller has to obtain the explicit and informed consent of all

⁴⁰ Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, p. 15, available at: <https://bit.ly/30QyFKd> Date of access: 22.12.2021.

⁴¹ EDPS and AEPD Joint Paper, 14 Misunderstandings with Regard to Identification and Authentication, June 2020.

⁴² EDPS and AEPD Joint Paper, 14 Misunderstandings with Regard to Identification and Authentication, June 2020. For more information see article: The Hidden Data in Your Fingerprints, available at: <https://bit.ly/38w7XH2> Date of access: 01.09.2021.

⁴³ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 80, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

⁴⁴ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 82, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

data subjects before using this biometric system. The system would be unlawful if it captures visitors or passers-by who have not consented to the creation of their biometric template, even if their template is deleted within the shortest possible period.⁴⁵

Multi-modal biometrics⁴⁶ can be defined as the combination of different biometric technologies to enhance the accuracy or performance of the system (it is also called multilevel biometrics). Biometric systems use two or more biometric traits/modalities from the same individual in the matching process. These systems can work in different ways, either collecting different biometrics with different sensors or by collecting multiple units of the same biometric. Some studies include within this category also systems working by performing multiple readings of the same biometric or those using multiple algorithms for feature extraction on the same biometric sample. Multimodal systems can minimise the dangers of fraud and help overcome difficulties caused by poor data quality or missing data but also increase ethical concerns, as they enable more efficient public surveillance.⁴⁷

2.3. RISKS AND THREATS RELATED TO BIOMETRIC DATA PROCESSING

The processing of sensitive data can bring great benefits and at the same time also has the potential to adversely affect fundamental rights, and carries a high risk of harm to individuals. The rapid development of technology poses risks for the processing of sensitive data.⁴⁸ Biometric data may reveal information about a person's state of health or his or her racial or ethnic background, as well as can produce risks of identity theft.⁴⁹ Consequently, such data requires enhanced protection.⁵⁰

For instance, systems analysing the face of a person as well as systems that analyse the DNA of a person can contribute very efficiently to the fight against crimes and efficiently reveal the identity of an unknown person suspected of a serious crime. However, these systems used on a large scale produce serious side effects. In the case of facial recognition where biometric data can be easily captured without the knowledge of the data subject, widespread use would terminate anonymity in public spaces and allow consistent tracking of individuals.⁵¹

⁴⁵ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 83, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

⁴⁶ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁴⁷ Ch. Wendehorst, Y. Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, 2021, p.14, available at: <https://bit.ly/30QyFKd> Date of Access: 22.12.2021.

⁴⁸ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford University Press, 2020, p. 370.

⁴⁹ Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, p. 2.

⁵⁰ Handbook on European data protection law, 2018, p. 96-97, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁵¹ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

Taking into account the fact that biometric technologies cannot ensure full accuracy, there is always an implicit risk coming from incorrect identifications. Such false positives can result in decisions affecting individual rights.⁵² In addition, one of the most serious risks is the theft of a biometric database or access to the data by an unauthorized person(s), which could cause significant damages.

In addition to privacy issues, there are also risks related to the possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying.⁵³ The bias of age, gender, and ethnicity in facial recognition systems threatens to reinforce the prejudices of society.⁵⁴

Reference should be made to the profiling⁵⁵ in the context of taking automated decisions or predicting behaviour or preferences in a specific situation. Information about an individual may be used for targeting and profiling purposes but also end up in discrimination, stigmatization.⁵⁶

2.4. STANDARDS OF BIOMETRIC DATA PROCESSING

The legal framework of the Council of Europe leaves it to domestic law to lay down appropriate protections for using sensitive data.⁵⁷ In this case, the conditions provided by Article 6 of Modernised Convention 108 shall be fulfilled. In particular, that appropriate safeguards in national law shall comply with the other provisions of the Convention. As for the EU law, Article 9 of the GDPR contains a detailed regime for processing special categories of data.⁵⁸

According to the Directive 2016/680, processing of biometric data for the purpose of uniquely identifying a person is allowed only when there is a strict need for it, adequate guarantees of protection of the rights and freedoms of the data subject are provided and one of the following situations exists:

- ➔ The processing is authorised by Union or Member State Law;
- ➔ The processing serves to protect the vital interests of the data subject or other natural person;
- ➔ Processing refers to data that has been publicly disclosed by the data subject.⁵⁹

⁵² Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁵³ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, p. 5, available at: <https://bit.ly/3kFg7nN> Date of access: 02.09.2021.

⁵⁴ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, p. 6, available at: <https://bit.ly/3kFg7nN> Date of access: 02.09.2021.

⁵⁵ According to article 4(4) of General Data Protection Regulation, profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

⁵⁶ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁵⁷ 108+ Convention, article 6.

⁵⁸ Handbook on European data protection law, 2018, p. 159-160, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁵⁹ 2016/680 Directive, article 10.

2.4.1. THE PRINCIPLE OF LAWFULNESS, FAIRNESS AND TRANSPARENCY OF PROCESSING

EU and Council of Europe data protection legislation sets out the obligation for the lawfulness, fairness and transparency of personal data processing.⁶⁰

According to the General Data Protection Regulation, the processing of biometric data requires the explicit consent⁶¹ of the data subject or another legitimate ground provided in the data protection legislation. For instance, processing special categories of data is allowed when processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.⁶²

As for the principle of fairness, it can be said that it basically regulates the relationship between the data controller and the data subject and it could also be linked to processing personal data in an ethical manner.⁶³ The principle of transparency establishes an obligation for the controller to take any appropriate measure to keep the data subjects informed about how their data are being used.⁶⁴

In many cases in which biometric data are processed, without a valid alternative like a password or a swipe card, the consent could not be considered as freely given. For instance, a system that would discourage data subjects from using it (e.g. too much time wasted for the user or too complicated) could not be considered as a valid alternative and then would not lead to valid consent.⁶⁵

Consent is only valid when sufficient information on the use of biometric data is given. Since biometric data may be used as a unique and universal identifier providing clear and easily accessible information on how the specific data are used is to be regarded as absolutely necessary to guarantee fair processing. Therefore this is a crucial requirement for valid consent in the use of biometric data.⁶⁶

When consent is required by Article 9 of the GDPR, the data controller shall not condition the access to its services to the acceptance of the biometric processing. In other words and notably when the biometric processing is used for authentication purposes, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data is impossible, disability situation making it difficult to use, etc.).⁶⁷

⁶⁰ 108+ Convention, article 5(3); General Data Protection Regulation, article 5(1)(a). 2016/680 Directive Preamble, par. 26, article 4(1)(a).

⁶¹ General Data Protection Regulation, article 9(2)(a).

⁶² General Data Protection Regulation, article 9(2)(g).

⁶³ Handbook on European data protection law, 2018, p. 119, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁶⁴ General Data Protection Regulation, article 12.

⁶⁵ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁶⁶ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁶⁷ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 86, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

2.4.2. PURPOSE LIMITATION PRINCIPLE

A prerequisite to using biometrics is a clear definition of the purpose for which the biometric data are collected and processed. Biometric data can for example be collected to ensure or increase the security of processing systems by implementing appropriate measures to protect personal data against unauthorised access.⁶⁸

Purpose limitation is one of the fundamental principles in European data protection law. According to the GDPR, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.⁶⁹ A similar approach is provided by the Modernised Convention 108.⁷⁰ Both documents set out exemptions relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Photographs on the internet, in social media, in online photo management or sharing applications may not be further processed to extract biometric templates or enroll them into a biometric system to recognise the persons on the pictures automatically without a specific legal basis (e.g. consent) for this new purpose. If there is a legal basis for this secondary purpose the processing must also be adequate, relevant and not excessive in relation to that purpose.⁷¹

The principle of purpose limitation is also set out by Directive 2016/680.⁷² However, the processing by the same or another controller for any of the purposes⁷³ set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:

A) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

B) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.⁷⁴

There is a strong connection between transparency and purpose limitation. When the purpose is specific and clear, individuals will know what to expect. The level of transparency and legal certainty is enhanced. At the same time, clear delineation of the purpose is important to enable data subjects to effectively exercise their rights, such as the right to object to processing.⁷⁵

⁶⁸ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁶⁹ General Data Protection Regulation, article 5(1)(b).

⁷⁰ 108+ Convention, article 5(4)(b).

⁷¹ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁷² 2016/680 Directive, article 4(1)(b).

⁷³ Those purposes are the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

⁷⁴ 2016/680 Directive, article 4(2).

⁷⁵ Handbook on European data protection law, 2018, p. 122-123, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021; ARTICLE 29 Data Protection Working Party, Opinion 3/2013 on purpose limitation, WP 203, 2 April 2013, available at: <https://bit.ly/32fLyhl> Date of access: 21.07.2021.

The processing of personal data for undefined and/or unlimited purposes, just based on the consideration that they may be useful in the future, is unlawful. The legitimacy of processing personal data will depend on the purpose of the processing, which must be explicit, specified and legitimate.⁷⁶

2.4.3. THE PRINCIPLE OF DATA MINIMISATION

Data processing must be limited to what is necessary to fulfill a legitimate purpose and should only take place when the purpose of the processing cannot be reasonably achieved by other means. Data processing may not disproportionately interfere with the interests, rights and freedoms at stake.⁷⁷

A specific difficulty may arise as biometric data often contain more information than necessary for matching functions. The principle of data minimisation has to be enforced by the data controller. Firstly, this means that only the required information and not all available information should be processed, transmitted or stored. Second, the data controller should ensure that the default configuration promotes data protection, without having to enforce it.⁷⁸

Personal data undergoing processing shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.⁷⁹ The categories of data chosen for processing must be necessary to achieve the declared overall aim of the processing operations, and a controller should strictly limit the collection of data to such information as is directly relevant for the specific purpose pursued by the processing.⁸⁰

2.4.4. THE PRINCIPLE OF DATA ACCURACY

According to the GDPR, personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.⁸¹ The principle of data accuracy is reinforced by the Modernised Convention 108⁸² as well as Directive 2016/680.⁸³

⁷⁶ Handbook on European data protection law, 2018, p. 122-123, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁷⁷ Handbook on European data protection law, 2018, p. 125, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁷⁸ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁷⁹ 108+ Convention, article 5 (4)(c); General Data Protection Regulation, article 5(1)(c). 2016/680 Directive, article 4(1)(c).

⁸⁰ Handbook on European data protection law, 2018, p. 125, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁸¹ General Data Protection Regulation, article 5(1)(d).

⁸² 108+ Convention, article 5(4)(d).

⁸³ 2016/680 Directive, article 4(1)(d).

2.4.5. LIMITING THE STORAGE PERIOD OF BIOMETRIC DATA

According to the GDPR, the Modernised Convention 108 and Directive 2016/680, personal data “shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data” are processed.⁸⁴ The processing of personal data for an indefinite or unlimited period is a violation of the law.⁸⁵

The controller should determine a retention period for biometric data that should not be longer than is necessary for the purposes for which the data were collected or for which they are further processed. The controller must ensure that the data, or profiles derived from such data, are permanently deleted after that justified period.⁸⁶

Example: an employer operates a biometric system to control access to a restricted area. An employee's role no longer requires him/her to access the restricted area (e.g. changes responsibility or job). In this case, his/her biometric data must be deleted since the purpose for which they were collected no longer applies.⁸⁷

2.4.6. ENSURING THE SECURITY OF BIOMETRIC DATA

Regarding biometric data, security should be a primary concern because biometric data are irrevocable. A breach concerning biometric data threatens the further safe use of biometrics as an identifier and the right to data protection of the concerned persons for which there is no possibility to mitigate the effects of the breach.⁸⁸ The risks increase with the number of applications using such data in order to identify a person. The more biometric data is used, the more likely biometric data theft will occur.⁸⁹

Considering that biometric authentication is like using the same password on many different accounts, which cannot be changed (face image, fingerprint, etc.), breach of data security for once is already a serious risk as the data processor will be able to access other accounts with this type of authentication system.⁹⁰ It can be said that similar cases have happened many times already.⁹¹

The principle of data security requires that appropriate technical or organizational measures be taken when processing personal data to protect it from unauthorised or unlawful processing and against

⁸⁴ General Data Protection Regulation, article 5(1)(e); 108+ Convention, article 5(4)(e); 2016/680 Directive, article 4(1)(e).

⁸⁵ Handbook on European data protection law, 2018, p. 122, available at: <https://bit.ly/34AFLUM> Date of access: 21.07.2021.

⁸⁶ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁸⁷ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁸⁸ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁸⁹ Opinion 3/2012 on developments in biometric technologies, available at: <https://bit.ly/2W6MtgT> Date of access: 21.07.2021.

⁹⁰ EDPS and AEPD Joint Paper, 14 Misunderstandings with Regard to Identification and Authentication, June 2020.

⁹¹ For more information see an article, available at: <https://bit.ly/2WzIFqi> Date of access: 31.08.2021.

accidental loss, destruction or damage, using appropriate technical or organisational measures.⁹² Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.⁹³

To ensure data security while creating a new product or service, it is important to adopt “privacy by design” and “privacy by default” approaches. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.⁹⁴

According to the GDPR, the controller is obliged to carry out an impact assessment where processing is likely to result in a high risk to the rights and freedoms of individuals given the category, volume, context and purposes of data processing, and in particular the use of new technologies.⁹⁵ A similar approach is set out in Directive 2016/680.⁹⁶

According to the GDPR, data protection impact assessments are crucial when personal data are processed for making decisions concerning natural persons, following any systematic and extensive evaluation of personal aspects relating to the individuals; processing involves the large-scale, systematic monitoring of publicly accessible areas; also, when sensitive data are processed on a large scale.⁹⁷

Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for the storage of the data.⁹⁸ In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or – when needed for specific purposes and in presence of objective needs – stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location. If the data controller cannot avoid having access to the templates, he must take appropriate steps to ensure the security of the data

⁹² General Data Protection Regulation, article 5(1)(f); 108+ Convention, article 7; 2016/680 Directive, article 4(1)(f).

⁹³ General Data Protection Regulation, article 32(1).

⁹⁴ General Data Protection Regulation, article 25(2).

⁹⁵ General Data Protection Regulation, article 35.

⁹⁶ 2016/680 Directive, article 27.

⁹⁷ Id, article 35(3).

⁹⁸ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 88, available at <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

stored. This may include encrypting the template using a cryptographic algorithm.⁹⁹

In any case, the controller shall take all necessary precautions to preserve the availability, integrity and confidentiality of the data processed. To this end, the controller shall notably take the following measures: compartmentalize data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature) and prohibit any external access to the biometric data. Such measures will need to evolve with the advancement of technologies.¹⁰⁰

Besides, if there is no longer a lawful basis for the processing, the raw data has to be deleted.¹⁰¹ Indeed, insofar as biometric templates derive from such data, one can consider that the constitution of databases could represent an equal if not an even bigger threat. It may not always be easy to read a biometric template without the knowledge of how it was programmed, whereas raw data will be the building blocks of any template. The controller must also delete biometric data and templates in the event of unauthorized access to the read-comparison terminal or storage server and delete any data not useful for further processing.¹⁰²

According to the Modernised Convention 108, Directive 2016/680 and the GDPR, the controller shall notify the personal data breach to the supervisory authority if the personal data breach is likely to result in a risk to the rights and freedoms of natural persons.¹⁰³ The obligation to notify is also imposed with regard to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject.¹⁰⁴

⁹⁹ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 88, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

¹⁰⁰ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 89, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

¹⁰¹ Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 90, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

¹⁰² Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 90, available at: <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.

¹⁰³ 108+ Convention, article 7(2); General Data Protection Regulation, article 33(1). 2016/680 Directive, article 30(1).

¹⁰⁴ 108+ Convention, article 7(2); General Data Protection Regulation, article 34(1). 2016/680 Directive, article 31.

2.4.7. THE PRINCIPLE OF ACCOUNTABILITY

Accountability requires controllers and processors to actively and continuously implement measures to promote and safeguard data protection in their processing activities.¹⁰⁵ This principle is set out in the GDPR,¹⁰⁶ Directive 2016/680¹⁰⁷ and Modernised Convention 108.¹⁰⁸

In the opinion of the Article 29 Working Group, the essence of accountability is determined by the responsibilities of the data controller:

- ➔ to implement appropriate and effective measures to ensure that the data protection principles and obligations are respected during the processing procedures;
- ➔ to provide documentation proving to data subjects and oversight authorities that measures have been taken to comply with data protection rules.¹⁰⁹

2.5. PROCESSING OF DATA IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY

The processing of personal data by a natural person in the course of a purely personal or household activity does not fall within the scope of the GDPR and Modernised Convention 108 and a person is not considered to be a data controller.¹¹⁰

An example of such kind of processing is the decision by a property owner to use a biometric system to control access of him or herself, members of the family and possibly third persons to a private home. In such a case, the means of data processing (system selection) and the purposes are determined by the property owner. However, if the biometric system is connected to a central device operated by the security services, the decision is made not only by the owner but also by third parties.¹¹¹ Consequently, this kind of processing of personal data will no longer be considered done in the course of purely personal or household activities and the exemption may no longer apply.

In case a biometric system is installed in a car, exclusively owned and used by a natural person, who decides to use the car and the system for purely personal activities, the collection and the use of biometric data would also fall under this exemption. If the car, however, would be owned by a company

¹⁰⁵ Handbook on European data protection law, 2018, p. 134.

¹⁰⁶ General Data Protection Regulation, article 5(2).

¹⁰⁷ 2016/680 Directive, article 4(4).

¹⁰⁸ 108+ Convention, article 10(1).

¹⁰⁹ Handbook on European data protection law, 2018, p. 136-137. ARTICLE 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability, available at: <https://bit.ly/3wLR46j>. Date of access: 13.11.2021.

¹¹⁰ General Data Protection Regulation, recital 18 and article 2(2)(c); 108+ Convention, article 3 (2).

¹¹¹ Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, 2013, p. 120.

and leased to its employees, and the car is equipped with a biometric access control system, this exemption may no longer apply.

The same would apply to fingerprint systems embedded in a laptop or mobile phone. If the laptop or mobile phone would be provided by, for example, an employer, the use of the laptop or mobile phone will in principle not be used in the course “of a purely personal or household activity”¹¹² and data protection rules will be fully applied to it.

¹¹² Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, 2013, p. 120-121.



3. PROCESSING OF GENETIC DATA

3.1. THE CONCEPT OF GENETIC DATA

According to the Recommendation No. R(97)5 on the Protection of Medical Data adopted in 1997,¹¹³ “genetic data” refers to all data, of whatever type, concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals.

The Article 29 Working Party adopted the Document on Genetic Data,¹¹⁴ outlining the basic characteristics of genetic data and emphasizing the importance of their legal protection. The Personal Data Protection Directive 95/46¹¹⁵ in force at the time did not mention genetic data and did not separate it from other data.¹¹⁶

Later, genetic data were included among special categories of data in the General Data Protection Regulation, which entered into force in 2018 and replaced the above-mentioned Directive. Modernised Convention 108 also defines genetic data as a special category of data.¹¹⁷

The definition of genetic data reflected in GDPR includes not only inherited but also acquired genetic characteristics. In particular, according to Article 4 of the Regulation, genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.¹¹⁸ According to the recital of GDPR, genetic data is obtained from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.¹¹⁹

Such definition of genetic data is detailed, though based on general terms so that it does not become obsolete under conditions of technological development and retain flexibility. Since it has already become possible to diagnose genetic disorders based on facial image analysis using computer imaging and in-depth learning algorithms, the last sentence of the definition set out in article 4, which says that genetic data is only personal data obtained from the analysis of a biological sample of an individual, is not accurate anymore.¹²⁰ In this case, the wider application of Article 4 is provided by

¹¹³ Available at: <https://bit.ly/3wswqll> Date of access: 09.11.2021.

¹¹⁴ Available at: <https://bit.ly/3bTFsVd> Date of access: 09.11.2021.

¹¹⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

¹¹⁶ Special categories of personal data include health-related data, which considerably overlaps genetic data, however, the latter is still different from the health data (for example, in terms of its importance in the future) due to certain aspects and its peculiarities.

¹¹⁷ 108+ Convention, article 6(1).

¹¹⁸ General Data Protection Regulation, article 4(13).






¹¹⁹ General Data Protection Regulation, recital 34.

¹²⁰ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, The EU General Data Protection Regulation, A Commentary, Oxford University Press, 2020, p. 201.

recital 34, according to which genetic data are also obtained from the analysis of other elements.¹²¹

Directive 2016/680,¹²² which deals with the processing of personal data by law enforcement agencies, defines genetic data in the same way as the General Data Protection Regulation.

The Article 29 Working Party emphasized several characteristics of genetic data which can be summarised as follows:

-  Genetic information is unique and distinguishes an individual from other individuals;
-  It may reveal information about that individual's blood relatives (biological family) including those in succeeding and preceding generations;
-  Genetic data can characterise a group of persons (e.g. ethnic communities);
-  Genetic information is often unknown to the bearer him/herself and non-modifiable;
-  Genetic data can be easily obtained or be extracted from raw material although this data may at times be of dubious quality.¹²³

Some parts of this definition are inaccurate. The statement that genetic information is unique somewhat diminishes the fact that the vast majority of human genes are identical, with only a small fraction of the difference. However, it is quite enough to distinguish one person from another. Also, references to the unchanging nature of genetic data ignore recent progress in making changes to the genome and the fact that diseases and their treatment can often alter DNA characteristics.¹²⁴

According to the Recommendation of the Committee of Ministers to member States on the protection of health-related data¹²⁵ and Explanatory Report of the Modernised Convention 108,¹²⁶ genetic data are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development.¹²⁷ It should be noted that when developing the definition of genetic data in GDPR, instead of the genetic characteristics acquired at the stage of prenatal development, the acquired genetic characteristics were selected for the very reason that genetic data can be changed after birth.¹²⁸

¹²¹ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation, A Commentary*, Oxford University Press, 2020, p. 201.

¹²² 2016/680 Directive Preamble, par. 23, Article 3(12).

¹²³ ARTICLE 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004, p. 4-5, available at: <https://bit.ly/3yRs26O> Date of access: 18.10.2021.

¹²⁴ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation, A Commentary*, Oxford University Press, 2020, p. 198.

¹²⁵ Available at: <https://bit.ly/3D7TQW0> Date of access: 09.11.2021.

¹²⁶ 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, par. 57, available at: <https://bit.ly/3oi32B4> Date of access: 09.11.2021.

¹²⁷ G. Gogichadze, A. Gedenidze, J. Tchumburidze, Pre-birth period, *Georgian-English-Russian-Latin Explanatory Dictionary of Medical Terminology* Tbilisi, 2009, p. 496.

¹²⁸ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation, A Commentary*, Oxford University Press, 2020, p. 199.

The genetic data defined by the GDPR include only those genetic characteristics of the individual that provide unique information about a person's health and physiology. Consequently, not all types of information obtained from biological sample analysis are included in the definition. The definition may not include human phenotypic characteristics (e.g., hair or eye color) or characteristics that distinguish one individual from another based on health status or physiology.¹²⁹

Whether or not physiological traits are included in genetic data definition depends entirely on how "genetic characteristics" are defined, which is largely equated with the term "genetic inheritance," and it usually refers to an individual's chromosomes and genes.¹³⁰ The processing of data that only concerns the phenotypic features of an individual (e.g. the mere taking/storing of a photograph of the individual) would normally not concern the processing of "genetic data" within the meaning of the GDPR. This is also supported by recital 51 of the GDPR, which states that "the processing of photographs should not systematically be considered to be processing of special categories of personal data".¹³¹ Besides, any biological material from which genetic data are derived is not in itself personal data.¹³²

In general, genetic and health data significantly overlap each other, although the difference is that genetic information may be about a person's future state of health. A special feature of genetic data is also the fact that this data can reveal information about the whole family of the data subject and his/her descendants. It is because of these characteristics that genetic data has become a separate subject of protection over time.

3.2. AREA OF THE USE OF GENETIC DATA, RISKS AND THREATS ASSOCIATED WITH THEIR PROCESSING

The area of application of genetic data is quite wide and is growing more and more with technological progress. Genetic data reveals a huge amount of information about a person, including a person's susceptibility to genetic disease, which plays a major role in research on rare genetic diseases and finding ways to treat them.¹³³ Besides the research benefits, the use of genetic data in the field of health is of immense importance: it can improve prevention, diagnosis, and treatment of disease, it also can be used to identify risk factors for adverse reactions to certain medications and prevent the adverse reaction.¹³⁴

¹²⁹ Id, p. 202.

¹³⁰ Id, p. 203.

¹³¹ Id.

¹³² Id. P. 202.

¹³³ John Paul M. Gaba, Joan Janneth M. Estremadura, Data Protection of Biometric Data and Genetic Data, *Ateneo Law Journal* 64, no. 3, February 2020, p. 967.

¹³⁴ Kristi Harbord, *Genetic data privacy solutions in the GDPR*, 7 *Tex. A&M L. Rev.* 269 (2019), p. 276.

Genetic data is also used in investigations (for example, to identify the offender), in family disputes, when it comes to adoption, paternity/maternity or guardianship and custody disputes. States use genetic data in immigration matters to establish family ties.¹³⁵ At the same time, the threat of genetic discrimination in the field of real estate and commercial transactions is growing. There are risks that various companies, such as individuals with a genetic predisposition to Alzheimer's disease, may refuse to rent property or lend money in exchange for real estate.¹³⁶

DNA information of individuals is also stored in national databases. This is presently mostly done by law enforcement authorities, often under the control of a judge. While the originally planned databases were often scheduled to be used for identification of (child) sex offenders, the scope of the databases have in most cases enlarged to include also DNA of persons and related to other serious criminal offences, further to anti-terrorism legislation, and sometimes even to other (minor) crimes.¹³⁷

Genetic data may be processed for the purposes of humanitarian crisis or action when proper legislative guarantees exist. A humanitarian crisis means an event or series of events that pose a critical threat to the health, safety, security or wellbeing of a community or other large group of people, authorities and humanitarian organisations may need to process genetic data for the reestablishment of family links or the identification of human remains.¹³⁸

Genetic data is used in the private sector, for example, in the genetic testing of consumers by private companies. In this case, users send DNA samples directly to companies that report their genetic information via the web or in writing. Consumers can address this type of private companies for genetic testing for a variety of reasons. Most often the request is related to the examination of information about their health, origin and genealogy. Some people seek primarily to find blood relatives or to identify the birth parents of a child who was adopted.¹³⁹

In addition, genetic data can be used in the private sector in the areas of employment and insurance, which poses a serious risk of genetic discrimination. Because of these risks, the use of genetic data for insurance and employment decisions is unacceptable.

When processing genetic data, data subjects may face serious risks, which makes it necessary to equip the subject with appropriate protection guarantees. Genetics technology has developed rapidly and with the changes in processes, alongside with the reduction in the costs of analysis, genome sequencing has become commonplace and the number of large databases is growing. All the above-mentioned suggest that the use of this technology is posing challenges in the data protection field that require ongoing monitoring.¹⁴⁰

¹³⁵ Ellen W. Clayton, Barbara J. Evans, James W. Hazel, Mark A. Rothstein, *The law of genetic privacy: applications, implications, and limitations*, Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, p. 22-24.

¹³⁶ *Id.*, p. 26.

¹³⁷ Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, Springer Dordrecht Heidelberg New York London, 2013, par. 371, p. 208.

¹³⁸ The explanatory memorandum to Recommendation [CM/Rec\(2019\)2](#) of the Committee of Ministers to member States on the protection of health-related data, par. 75.

¹³⁹ Ellen W. Clayton, Barbara J. Evans, James W. Hazel, Mark A. Rothstein, *The law of genetic privacy: applications, implications, and limitations*, Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, p. 16.

¹⁴⁰ Explanatory memorandum to Recommendation [CM/Rec\(2019\)2](#) of the Committee of Ministers to member States on the protection of health-related data, par. 69.

3.3. THE PRINCIPLE OF PROHIBITION OF DISCRIMINATION AND STIGMATIZATION ON GENETIC GROUNDS

The principle of prohibition of discrimination and/or stigmatization in the processing of genetic data is reinforced by a number of important international legal instruments. The recitals of the General Data Protection Regulation, focus on the risks of discrimination.¹⁴¹ The Modernised Convention 108 allows the processing of special categories of data only in the presence of appropriate guarantees enshrined in law, which should ensure the protection of human rights and fundamental freedoms, especially avoid the risk of discrimination.¹⁴²

Convention on Human Rights and Biomedicine of the Council of Europe is the first document that was created to protect the dignity of all humans and respect for their rights and fundamental freedoms with regard to the application of biology and medicine. The Convention stipulates that a choice between the interests of society and science and the well-being and interests of humans must necessarily be made in favor of the latter. Genetic testing that reveals information about a genetic disease or a predisposition or susceptibility to the latter may become a means of discrimination and selection, which is why the Convention sets out the principle of prohibition of discrimination on the basis of genetic heritage.¹⁴³

Additional Protocol to the Convention that applies to genetic tests, which are carried out for health purposes, also prohibits discrimination against a person or group of people on the grounds of genetic heritage and indicates the need to take appropriate measures to avoid stigmatization related to genetic characteristics.¹⁴⁴ The Additional Protocol separates stigmatization and discrimination from each other. As stated in the Explanatory Report, stigmatization is not necessarily related to the realization of a person's rights and implies common beliefs about the genetic characteristics of a person or group of persons. These beliefs may also reflect the truth, although they place negative labels on a person or group of persons. Possible measures required by the Additional Protocol to prevent stigmatisation include general information campaigns on the human genome and its characteristics and on advances in our knowledge of human genetics.¹⁴⁵

Particular risks of genetic discrimination may arise in the context of employment or insurance. Recommendation of the Committee of Ministers on the processing of personal data in the context of employment emphasizes that genetic data cannot be processed to determine the professional suitability of an employee or a job applicant, even with the consent of the data subject.¹⁴⁶

¹⁴¹ General Data Protection Regulation, recital 75 and 85.

¹⁴² 108+ Convention, article 6.

¹⁴³ Convention on Human Rights and Biomedicine of the Council of Europe, article 11.

¹⁴⁴ Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes, article 4.

¹⁴⁵ Explanatory Report to the Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes, Par. 42.

¹⁴⁶ Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, article 9(3).

The processing of genetic data in the context of employment may only be permitted if it is provided for by domestic law and subject to appropriate safeguards. Exceptional circumstances are, for example, the processing of genetic data to avoid any serious prejudice to the health of the data subject or third parties.¹⁴⁷ Another example is processing genetic data through a genetic monitoring programme that monitors the biological effects of toxic substances in the workplace, where the monitoring is required by law or, under carefully defined conditions, where the programme is voluntary.¹⁴⁸

Discrimination in the processing of genetic data for insurance purposes is, for example, the imposition of higher insurance taxes on individuals who are at increased risk of developing certain diseases. Recommendation of the Committee of Ministers on the processing of personal health-related data for insurance purposes establishes specific rules for avoiding genetic discrimination in the insurance process and prohibits predictive genetic tests for insurance purposes.¹⁴⁹

Existing predictive data resulting from genetic tests should not be processed for insurance purposes unless specifically authorised by law.¹⁵⁰ If so, their processing should only be allowed after assessment of conformity with particular conditions. Namely, personal data should only be processed if the processing purpose has been specified and the relevance of the data has been duly justified, the quality and validity of the data are in accordance with generally accepted scientific and clinical standards, data resulting from a predictive examination have a high positive predictive value and processing is duly justified in accordance with the principle of proportionality in relation to the nature and importance of the risk in question.¹⁵¹ Existing data from genetic tests from family members of the insured person should not be processed for insurance purposes in any case.¹⁵²

¹⁴⁷ Id.

¹⁴⁸ Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment and Explanatory memorandum, Par. 81.

¹⁴⁹ Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, principle 4.

¹⁵⁰ Id.

¹⁵¹ Id. par. 5 and 16.

¹⁵² Id. par. 17.

3.4. SCOPE, PRINCIPLES AND GROUNDS FOR GENETIC DATA PROCESSING

Rules enshrined in the Modernised Convention 108 and the General Data Protection Regulation do not apply to the processing of personal data by a natural person in the course of purely personal or household activities. Whether activities are “purely personal or household” will depend on the circumstances.¹⁵³ For example, when personal data is made available to a large number of persons or to persons external to the private sphere, (such as a public website on the internet) the exemption will not apply.¹⁵⁴

The Modernised Convention 108 and the General Data Protection Regulation apply to living individuals.¹⁵⁵ However, due to the specificity of the genetic data, personal data protection legislation may apply to the processing of a deceased person’s genetic data, as this data may disclose information about his or her living family members.

3.4.1. PRINCIPLES OF GENETIC DATA PROCESSING

Key Principles relating to the processing of personal data are enshrined in the Modernized Convention 108 and the General Data Protection Regulation: lawfulness, fairness and transparency of processing, purpose limitation, data minimization, accuracy, storage limitation, data security and accountability principles.¹⁵⁶

The principle of lawfulness means that there is a legal basis for data processing and it pursues a legitimate purpose. When a data subject consents to the processing of genetic data and the law does not prohibit the processing of such data with the consent of the person, then their processing may be considered lawful. Lawful processing also means that the processed data is not used for other purposes, processing is in accordance with the law, pursues a legitimate purpose and is necessary and proportionate to achieve that purpose.¹⁵⁷ For instance, the Spanish Data Protection Authority (DPA) deemed that the creation of a file of genetic samples to identify newborns through DNA testing, the aim of which would be to prevent mother-infant mismatches, would contravene the principle of proportionality since the same result could be reliably obtained with other means e.g. identity bracelets or footprints.¹⁵⁸

¹⁵³ 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, Par. 28.

¹⁵⁴ *Id.*

¹⁵⁵ 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, par. 30. General Data Protection Regulation, recital 27.

¹⁵⁶ 108+ Convention, articles 5, 6, 7 and 8. General Data Protection Regulation, article 5.

¹⁵⁷ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation, A Commentary*, Oxford University Press, 2020, p. 314.

¹⁵⁸ Article 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

Fair processing requires that the data be processed in accordance with the data subject's expectations. At the same time, the person should be alerted about potential risks. This issue is especially important when processing genetic data. **The principle of transparent** data processing is closely linked to informing a person. Data processing should be transparent and clear to the data subject. She/he should be informed not only about the risks of processing genetic data but also about the purposes of the processing, as well as about the right to refuse or withdraw consent. **The purpose limitation principle** requires data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.¹⁵⁹ Considering the complexity and the sensitivity of the genetic information there is a great risk of misuse and/or re-use of them or risks of re-use through additional analysis of the underlying material for various purposes.¹⁶⁰ To further process personal data it is necessary to have appropriate legal ground. Nevertheless, it provides for exemptions to the prohibition to further process data for historical, statistical or scientific purposes provided that appropriate safeguards are put in place.¹⁶¹ In this case, when the processing purposes allow it, the data subject should not be identifiable. According to Modernised Convention 108, genetic information reflected in the statistics must be anonymous, however, if the identity of the data subject is essential for processing, then an exception to this rule is permissible.¹⁶²

Genetic data processed with a preventive aim, for diagnosis or treatment of the data subject or a member of their biological family or scientific research should be used only for these purposes or to enable the persons concerned by the results of such tests to make an informed decision on these matters.¹⁶³

The principle of purpose limitation also applies to the processing of genetic data for the purposes of litigation or investigation. For example, when genetic data is processed to determine paternity, this information should only be used to establish a genetic link between the child and the father.¹⁶⁴

Data minimization principle requires that only such data shall be processed as are adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed.¹⁶⁵ Problematic in this regard is that the genetic information obtained during the investigation is often stored even after the person has been found not guilty.¹⁶⁶

The principle of data accuracy provides for the obligation to update data if necessary. Genetic test results may contain some errors, but if they are the results of a test with a significant margin of error,

¹⁵⁹ Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation, A Commentary*, Oxford University Press, 2020, p. 315.

¹⁶⁰ Article 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

¹⁶¹ General Data Protection Regulation, article 9(2)(j).

¹⁶² 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, par. 61.

¹⁶³ Recommendation [CM/Rec\(2019\)2](#) of the Committee of Ministers to member States on the protection of health-related data, par. 7.2.

¹⁶⁴ Explanatory memorandum to Recommendation [CM/Rec\(2019\)2](#) of the Committee of Ministers to member States on the protection of health-related data, par. 74.

¹⁶⁵ Handbook on European data protection law, 2018, p. 125-126.

¹⁶⁶ Privacy International, DNA and Genetic Data, available at: <https://bit.ly/3H8lJpF> Date of access: 19.10.2021.

so long as that margin of error is explained to the data subject, the data will be accurate.¹⁶⁷ If a conclusion about a genetic result is a matter of opinion, this should also be explained. Even if data are updated, it could be that earlier 'inaccuracies' should be retained as an accurate record of the analytical or decision-making process.¹⁶⁸

According to the **principle of storage limitation**, personal data must not be kept for any longer than is necessary. However, it is considered in accordance with this principle when data is stored anonymously or for scientific research. Typically, genetic data collected for research purposes should be anonymous if it is not against these purposes.

Regarding the principle of storage limitation, the European Court of Human Rights ruled that indefinite storage of fingerprints, cellular samples, and DNA profiles after the investigation against the suspect was terminated and in another case the suspect was acquitted, was not a necessary and proportionate measure in a democratic society.¹⁶⁹ Modernised Convention 108 allows exceptions, however, an exception must constitute a necessary and proportionate measure to pursue aims provided for by law.¹⁷⁰

The results of DNA analysis and information obtained in criminal proceedings should be deleted after the purpose for which it was kept has been achieved. The results of DNA analysis and the information so derived might, however, be retained where the individual concerned has been convicted of serious offences against the life, integrity or security of persons. In any case, strict storage periods should be defined by domestic law.¹⁷¹

The obligation to protect security and confidentiality during data processing is established by the principle of **data security**.¹⁷² This means that the controller and the processor, should take specific technical and organisational measures, such measures could include pseudonymising and encrypting personal data, keeping certain data separate, notifying supervisory authorities or data subjects, when there is a risk of breach.

Recommendation of the Committee of Ministers on the processing of personal data in the context of employment explains that, where their processing is lawful and where appropriate, genetic data, should be stored separately from other categories of personal data held by employers. It is important to take technical and organizational security measures to prevent persons who do not belong to the employer's medical service from having access to the data.¹⁷³ Also, personal information collected

¹⁶⁷ PHG Foundation, GDPR and Genomic Data, p. 94.

¹⁶⁸ Id.

¹⁶⁹ European Court of Human Rights judgment of 2008 4 December, S. and Marper v. the United Kingdom.

¹⁷⁰ 108+ Convention, article 11(1).

¹⁷¹ COM Recommendation 1992A: Committee of Ministers of the Council of Europe, 'Recommendation on the Use of Analysis of Deoxyribonucleic Acid (DNA) within the Framework of the Criminal Justice System' (R (92)1, 10 February 1992), par. 8 .

¹⁷² 108+ Convention, article 7; General Data Protection Regulation, article 5(1)(f).

¹⁷³ Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, explanatory report, par. 9.6.

during biological material research should be kept confidential.¹⁷⁴ Researchers should only have access to human biological materials or data that are coded or anonymised, and researchers should be required to not attempt to re-identify participants, except in exceptional cases.¹⁷⁵ There should be an obligation to keep genetic data separate when conducting genetic testing for health purposes. However, in the case of a severe genetic risk for other family members, the obligation to protect professional secrecy and confidentiality may be limited.¹⁷⁶

EU directive, which lays down the rules for the processing of personal data by law enforcement agencies, also obliges the Member States to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data.¹⁷⁷

According to the **principle of accountability**, controllers and processors are responsible for compliance of their processing operations with data protection law and their respective obligations. This principle envisages recording processing activities, undertaking data protection impact assessments, ensuring data protection by design and by default, and implementing other measures.¹⁷⁸

The Article 29 Working Party regarding the use of bio-banks clarified that to ensure a high level of security, data controllers should carry out surveys of potential risks, establish policies for security, inform and train staff.¹⁷⁹

For instance, according to Directive 2016/680, Member States shall provide for controllers to maintain a record of all categories of processing activities under their responsibility, including information about the controller, purposes of the processing, the categories of the data subject and the categories of personal data; legal basis; the envisaged time limits for erasure of the different categories of personal data, where possible; the use of profiling, etc.¹⁸⁰ A similar obligation is set out in the General Data Protection Regulation.¹⁸¹

¹⁷⁴ Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, explanatory report, par. 37.

¹⁷⁵ OECD Guidelines on Human Biobanks and Genetic Research Databases 7.D p.14

¹⁷⁶ Recommendation No. R (92) 3 of the Committee of Ministers to Member States on Genetic Testing and Screening for Health Care Purposes, principles 9 and 10.

¹⁷⁷ 2016/680 Directive, article 29.

¹⁷⁸ Handbook on European data protection law, 2018, p. 134-135.

¹⁷⁹ Article 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004, p. 11.

¹⁸⁰ 2016/680 Directive, article 24(1).

¹⁸¹ General Data Protection Regulation, article 30.

3.4.2. GROUNDS FOR GENETIC DATA PROCESSING

Modernised Convention 108 requires that the data processing should be carried out based on the free, specific, informed and unambiguous consent of the data subject or some other legitimate ground set out by law.¹⁸² Unlike the Convention, the General Data Protection Regulation provides a list of the grounds for processing special categories of data. According to the general rule established by the Regulation, the processing of special categories of data is prohibited, unless there are specific exceptions defined by the regulation. However, even in the case of exceptions, data shall be processed based on the law. One of the exceptions is the consent of the data subject.¹⁸³ It is the consent of the data subject that genetic companies conduct genetic testing to determine health-related genetic risks or origin issues.

Consent to genetic data processing is not required when it is aimed at identifying offenders within the scope of the investigation as well as enhancing the identification of missing persons. In this latter case, the ground for processing is to protect the vital interests of the data subject.¹⁸⁴ Directive 2016/680 provides for the protection of the vital interests of the data subject or other natural person as one of the grounds for the processing of special categories of data.¹⁸⁵ However, during civil suit procedures, where genetics are used to test the existence of paternal or other family links, explicit consent is required.¹⁸⁶ It is not allowed to steal genetic material and process data without the data subject's knowledge (For example, carrying out a genetic test to determine paternity by hair samples secretly taken from the father).¹⁸⁷

Legislation may prohibit the processing of special categories of data even if the data subject gives his/her consent. As already mentioned, such a prohibition regarding genetic data may be linked to the conduct of genetic prediction tests for employment or insurance purposes.

An important basis for the processing of genetic data is their processing for medical and public health purposes.¹⁸⁸ As already noted above, genetic data are often used to diagnose or treat diseases. It is possible to process personal data for public health objectives, such as separating human DNA from virus DNA as part of pathogen sequencing during the outbreak of different diseases, the aim of which is to study and better manage various infectious diseases.

Exceptions are also made to the processing of data for the purposes of archiving, scientific or historical research or the production of statistics. To ensure the protection of personal data, the genetic data used in medical or other scientific research must be anonymous. At the same time, if necessary for research purposes, it is also possible to process the genetic data of an identifiable person or

¹⁸² 108+ Convention, article 5(2).

¹⁸³ General Data Protection Regulation, article 9.

¹⁸⁴ Article 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

¹⁸⁵ 2016/680 Directive, article 10.

¹⁸⁶ Article 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004, p. 12.

¹⁸⁷ Id.

¹⁸⁸ General Data Protection Regulation, article 9(2)(h)(i).

group of individuals. The need to process health-related data for scientific research should be evaluated in light of the purposes of the research project, the risks to the data subject, and as concerns the processing of genetic data, in light of the risk to the biological family.¹⁸⁹

Other grounds for the processing of special category data defined by the Regulation are the protection of the vital interests of the data subject, use of these data by foundations or not-for-profit bodies in the course of their legitimate activities, disclosure of data by the data subject, fulfillment of legal obligations and protection of important public interest.

An example of the processing of genetic data to fulfill legal obligations can be considered the processing of genetic data for the purposes of the court proceedings. In this case, genetic data can be used in both civil (family disputes, establishing paternity/maternity) and criminal cases (for example, to identify a person). It is also possible for a data subject to publish genetic data on a website, for example, on an ancestry database, and thus make it available to all persons.¹⁹⁰ Genetic data can be used to protect the vital interests of the data subject, for instance, during natural disasters where the data subject is unable to provide consent and the genome sequencing is necessary to track a life-threatening disease.¹⁹¹

In addition, Article 9(4) of the General Data Protection Regulation indicates the possibility of Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

3.4.2.1. CONSENT OF THE DATA SUBJECT

The processing of genetic data is often based on the consent of the data subject. In addition to genetic testing, the use of genetic data in scientific research not so rarely is the result of consent. General Data Protection Regulation recital indicates that it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, therefore, data subjects should be allowed to give their consent.¹⁹²

According to General Data Protection Regulation, consent of the data subject must be voluntary, clearly expressed, free and informed.¹⁹³ At the same time, the data subject is entitled to withdraw his/her consent of which it is necessary to inform him/her.¹⁹⁴ To process special categories of data, consent must be given, in a clear and understandable manner, by a written or an oral statement.¹⁹⁵ The

¹⁸⁹ Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, par. 15.2.

¹⁹⁰ Colin Mitchell, Johan Ordish, Emma Johnson, Tanya Brigden and Alison Hal, *GDPR and genomic data*, 2020, p. 76.

¹⁹¹ *Id.*, p. 77.

¹⁹² General Data Protection Regulation, recital 33.

¹⁹³ *Id.*, article 4(11).

¹⁹⁴ *Id.*, article 7(3).

¹⁹⁵ *Id.*, recital 32.

Modernised Convention 108 indicates that consent must be given either by a statement or by a clear affirmative action.¹⁹⁶ Correspondingly, inactivity or pre-validated forms or boxes should not, therefore, constitute consent.¹⁹⁷

UNESCO's International Declaration on Human Genetic Data requires that adequate and appropriate information shall be provided to the person concerned in advance about the purposes for which human genetic data are being used and stored, if necessary, information should be given about the risks and consequences, also about the right to withdraw consent.¹⁹⁸ Prior, informed consent of the person for the collection of genetic data is required, however, certain exceptions may be determined by law. Free consent means that it is given without inducement by financial or other personal gains.¹⁹⁹ When a person withdraws consent, his/her stored genetic data should be destroyed. Human genetic data collected in the course of a criminal investigation, civil proceedings or forensic purposes should be destroyed when the aims for which the data were stored were achieved.²⁰⁰

It is important to note that any genetic testing should be accompanied by appropriate counseling concerning medical facts, the results of tests, as well as the consequences and choices.²⁰¹

3.5. THE RIGHT TO RECEIVE AND REFUSE TO RECEIVE INFORMATION

According to the law of EU and Council of Europe,²⁰² controllers are obliged to provide information about the planned processing to the data subjects when collecting their data. When processing genetic information, the right to receive information may also be extended to the family members of the data subject. The controller must proactively comply with the obligation to provide information, regardless of whether the data subject shows interest in the information or not.²⁰³ However, when processing genetic data, it is possible for the data subject to refuse to receive the information.

Directive 2016/680 establishes the rights of the data subject to be informed and have access to his/her personal data, however, it allows the possibility of restricting access in certain cases.²⁰⁴ In this

¹⁹⁶ 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, par. 42.

¹⁹⁷ Id.

¹⁹⁸ International Declaration on Human Genetic Data, article 6.

¹⁹⁹ Id, article 8.

²⁰⁰ Id, Article 21.

²⁰¹ Recommendation No. R (92) 3 of the Committee of Ministers to Member States on Genetic Testing and Screening for Health Care Purposes, 3rd principle.

²⁰² 108+ Convention, article 8; General Data Protection Regulation, recital 39, articles 12-14.

²⁰³ Handbook on European data protection law, 2018, p. 207.


²⁰⁴ For example, when access interferes with the interests of the investigation, it is necessary to protect public safety or the rights or freedoms of others, and so on.


case, the data subject must be informed about the reasons and grounds for the refusal.²⁰⁵

Convention on Human Rights and Biomedicine of the Council of Europe establishes the right to receive information about the health and genetic testing results of patients and also provides for the right of the patient to refuse to receive this information.²⁰⁶ A genetic test performed for health reasons may reveal information about a person or his/her family members that is not related to health (for example, the presence of an unexpected biological link). The convention leaves it to the Member States to regulate the issue of disclosure of such unexpected information to interested parties and establish appropriate rules/conditions.²⁰⁷ Upon making a decision, the wishes of the person, as well as the risks of harm to the person and his family members should be taken into consideration.²⁰⁸

Recommendation of the Committee of Ministers on the protection of health-related data provides for the right of the person to refuse to receive information when analysis may reveal unexpected findings or the data subject does not wish to know certain health aspects, everyone should be aware, prior to any analysis, of the possibility of not being informed of the results. For example, this situation may arise when the data subject does not want to find out if he or she carries the genes for a particular incurable genetic disease. However, this right may, in exceptional circumstances, have to be restricted notably in the data subject's interest or in light of the doctors' duty to provide care.²⁰⁹

The data subject and his/her biological family members have common genetic characteristics. Consequently, the results of genetic testing can be of great importance to them as well. The issue of sharing genetic information of a data subject with his/her biological relatives arises when this data is also relevant to their health and future. In such cases, family members may be given access to the information without the consent of the data subject. This can be done in two ways:

 Other family members could also be considered as "data subjects" or

 Based on the fact that their interests may be directly affected, family members would have the right to receive this information.²¹⁰

For instance, in Italy, in 1999, the father's right to privacy was overridden by the daughter's right to health. Although the father refused to disclose genetic information about him to his child, the latter was still granted access to that information.²¹¹ It should be noted that a person's right not to receive genetic information also applies to family members, which should be taken into account particularly if the disease is highly serious and there is no means to prevent or treat it.²¹²

²⁰⁵ 2016/680 Directive, article 15.

²⁰⁶ Convention on Human Rights and Biomedicine of the Council of Europe, article 10.

²⁰⁷ Explanatory Report to the Convention on Human Rights and Biomedicine of the Council of Europe, par. 130.

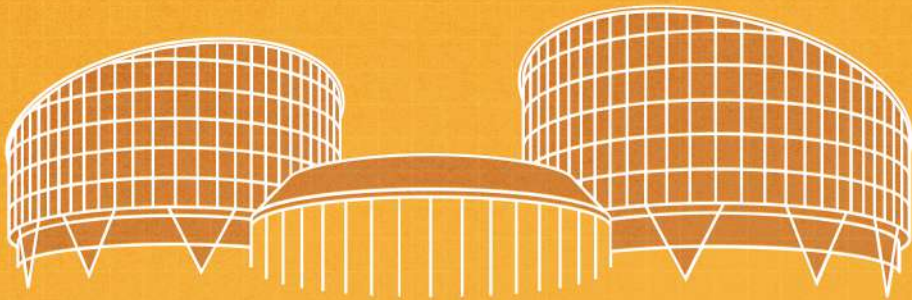
²⁰⁸ Id.

²⁰⁹ 7.6 par, available at: <https://bit.ly/3qqnULR> Date of access: 11.11.2021.

²¹⁰ Article 29 Data Protection Working Party, Working Document on Genetic Data, 17 March 2004.

²¹¹ Id, p. 9.

²¹² Id.



4. JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS

This chapter discusses judgments of the European Court of Human Rights related to the processing of biometric and genetic data.

4.1. S. AND MARPER V. THE UNITED KINGDOM

In the case of ***S. and Marper v. The United Kingdom***,²¹³ the European Court of Human Rights found that the retention of DNA profiles, cellular samples, and fingerprints of the persons who have been acquitted violated Article 8 of the European Convention on Human Rights.

THE CIRCUMSTANCES OF THE CASE

The first applicant was arrested at the age of 11 and charged with attempted robbery. His fingerprints and DNA samples were taken, however, eventually, he was acquitted. The second applicant – Mr. Marper was arrested for harassment of his partner. His fingerprints and DNA samples were also taken. Before a pre-trial review took place, Marper and his partner had reconciled. Therefore, the charge was not pressed and the case was formally discontinued. Both applicants asked for their fingerprints and DNA samples to be destroyed, but in both cases the police refused.

The applicants applied for judicial review of the police decisions. However, in March 2002 the Administrative Court rejected their application. In September 2002 the Court of Appeal upheld the decision of the Administrative Court, and in 2004 the House of Lords dismissed an appeal by the applicants.

Eventually, the applicants lodged applications with the European Court of Human Rights and complained that retention of their DNA profiles, cellular samples, and fingerprints, after the criminal proceedings against them had ended with an acquittal or had been discontinued, violated Articles 8 and 14 of the Convention.

THE COURT'S ASSESSMENT

In its judgment of 4 December 2008, the Court stated that retention of the DNA profiles, cellular samples, and fingerprints violated the applicants' right to respect for private and family life. In its assessment, the Court agreed with the respondent State that the retention of DNA profiles and fingerprints pursued the legitimate aim of the detection and, therefore, prevention of crime. However, the Court highlighted that interference is considered "necessary in a democratic society" if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued.

The Court stated that the cellular samples contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of

²¹³ Available at: <https://bit.ly/3n8AUB1> Date of access: 12.11.2021

great relevance to both the individual and his relatives. Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion.

Moreover, discussion on the differences between DNA profiles and fingerprints might be necessary; however, retention of both constitutes an interference with the right to respect for private life. The Court found it to be beyond dispute that DNA profiles are important for fighting against crime, nor is it disputed that states have made rapid and marked progress in using DNA information in the determination of innocence or guilt. The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests.

The Court observed that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. According to the judgment, the interference must pursue a legitimate aim, be in accordance with the law, and the law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.

Notably, the Court considered the issue in terms of the persons who had been suspected, but not convicted. The European Court took into account the fact that according to the UK legislation, the material might be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender. Moreover, the retention was not time-limited and there existed only limited possibilities for an acquitted individual to have the data removed from the national database or the materials destroyed. The Court noted that the retention of biological samples of those persons who had been acquitted could not be justified by the legitimate aim of prevention of a crime. According to the judgment, the respondent State overstepped any acceptable margin of appreciation that resulted in disproportionate interference with the applicants' right to respect for private and family life.

4.2. M.K. V. FRANCE (2013)

In the case of *M.K. v. France*,²¹⁴ the European Court of Human Rights found the violation of Article 8 of the European Convention on Human Rights as the retention of an innocent person's data for 25 years was not necessary in a democratic society.

THE CIRCUMSTANCES OF THE CASE

The police arrested M.K. for book theft and the investigating authorities took his fingerprints. By a judgment handed down in 2005, the Paris Court of Appeal acquitted the applicant. On 28 September 2005, the applicant was taken into police custody also for book theft and he was again fingerprinted. On 2 February 2006, the proceedings were discontinued by the Paris public prosecutor. The fingerprints taken during these proceedings were entered into the national fingerprint database. The applicant requested the removal of his fingerprints. The public prosecutor ordered the deletion only of the fingerprints taken during the first set of proceedings. He argued that retaining one specimen of the applicant's fingerprints was justified in the latter's interests, as it could rule out his involvement in acts committed by a third person stealing his identity.

The Paris Tribunal held that information about M.K. should remain in the database. The President of the Investigation Division of the Paris Court of Appeal upheld this order and the Court of Cassation dismissed an appeal.

The applicant lodged the application with the European Court of Human Rights and complained that Articles 8 and 6 of the Convention had been violated.

THE COURT'S ASSESSMENT

The European Court reiterated that the retention of fingerprints in connection with an identified or identifiable individual constitutes an interference with Article 8 and such interference must be in accordance with the law. The law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. According to the Court, similar to the case of *S. and Marper v. the United Kingdom*, in this case, the Court should determine whether the interference was “necessary in a democratic society.” The legitimate aim of collection, usage, and retention of personal data is the detection and, therefore, prevention of crime. Interference with the right must be proportional to the legitimate aim and must answer a ‘pressing social need.’

According to the judgment of the European Court, the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life. Therefore,

²¹⁴ Available at: <https://bit.ly/3kyp6pX> Date of access: 12.11.2021

the domestic law must afford appropriate safeguards to protect private life. The data must not be excessive in relation to the purposes for which they are stored, and preserved in a form that permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

The Court also highlighted the risk of stigmatization, stemming from the fact that persons in the applicant's position, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. The Court considered that accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant.

The European Court of Human Rights held that there has been a violation of Article 8 of the Convention and the retention for twenty-five years of the fingerprints of persons suspected of having committed offences but not convicted was not necessary in a democratic society.

4.3. GAUGHRAN V. THE UNITED KINGDOM (2020)

In the Case of *Gaughran v. the United Kingdom*,²¹⁵ the applicant's DNA profile, fingerprints, and photograph were retained in the police database without reference to the seriousness of the offence or the need for indefinite retention and in the absence of any real possibility of a review. The European Court of Human Rights found that there was a violation of Article 8 of the European Convention.

THE CIRCUMSTANCES OF THE CASE

In October 2008, the applicant was driving with excess alcohol. The Magistrate Court fined him with 50 pounds sterling and disqualified him from driving for 12 months. This offence was also punishable by imprisonment. No immediate or suspended custodial sentence was imposed on him, however, he was a convicted person. (His conviction was spent in 2013).

In 2009, the applicant's solicitor wrote to the Police Service of Northern Ireland (the "PSNI") claiming that the retention of the applicant's photograph, fingerprint, and a DNA sample was unlawful. He requested that they be destroyed or returned to the applicant. In 2015, the DNA sample was destroyed, however, DNA profile, fingerprints and photograph were still retained in the database. Challenging at the national level the refusal to erase personal data did not result in the desired outcome for Gaughran. He lodged the application with the European Court of Human Rights and complained that Article 8 of the Convention had been violated.

²¹⁵ Available at: <https://bit.ly/3HrOXd5> date of access: 12.11.2021

THE COURT'S ASSESSMENT

According to the judgment of 13 June 2020 of the European Court of Human Rights, retention of applicant's personal data for the legitimate aim of detecting crime violated the right to respect for private life. Similar to the above-discussed cases, in this judgment the Court indicated that retention of personal data constituted an interference with the right to respect for private life that pursued the legitimate aim of detecting crime. Such interference must be necessary in a democratic society.

The majority of member states of the Council of Europe had retention periods limited in time. The UK was among those few countries that had an indefinite retention period. Therefore, it had to justify the existence of efficient safeguards. The Court recalled the importance of examining compliance with the principles of Article 8 where the powers vested in the state are obscure, creating a risk of arbitrariness, especially where the technology available is continually becoming more sophisticated.

The judgment states that the case of ***S. and Marper v. the United Kingdom*** was different, as in this case, the identical risk of stigmatisation did not exist due to the conviction of the applicant. According to the Court, the biometric data of Gaughran were retained without reference to the seriousness of his offence and without regard to any continuing need to retain that data indefinitely. There was no provision allowing the applicant to apply to have the data concerning him deleted if conserving the data no longer appeared necessary in view of the nature of the offence, the age of the person concerned, the length of time that had elapsed, and the person's current personality.

According to the judgment, the United Kingdom overstepped the acceptable margin of appreciation and failed to strike a fair balance between the competing public and private interests. There has accordingly been a violation of Article 8 of the Convention.

4.4. P.G. AND J.H. V. THE UNITED KINGDOM (2001)

In the case of ***P.G. and J.H. v. The United Kingdom***,²¹⁶ the European Court of Human Rights ruled that secret surveillance by the police during investigation and installation of a covert listening device in the police station to obtain voice samples without the consent of the applicants constituted a violation of the right to respect for private life and correspondence guaranteed by the Convention.

THE CIRCUMSTANCES OF THE CASE

The police received information that an armed robbery of a cash-collection van was going to be committed by the first applicant and B. They installed a covert listening device in B's flat to obtain further details about the robbery. Covert surveillance measures were governed by the Home Office Guidelines and not by a legally binding act. At the same time, the police made a request to British Tele-

²¹⁶ Available at: <https://bit.ly/3kw16DX> Date of access: 12.11.2021.

communications for itemised billing in relation to the telephone number of B. Eventually, no robbery took place. The applicants were arrested and charged with conspiracy to commit armed robbery. The police wished to compare speech samples of the suspects with the tapes, however, the applicants refused to provide voice samples voluntarily. Therefore, the police installed a covert listening device in a police cell. During the proceedings, the court found all the evidence admissible, and due to the seriousness of the crime, considered that the interference with the privacy of the person was justified. Applications referred to the Court of Appeal were refused because of the absence of an arguable ground of appeal.

THE COURT'S ASSESSMENT

The European Court of Human Rights held that installing a covert listening device in a flat in the absence of domestic law regulating the use of covert listening devices violated the right to respect for private life. Such measures were governed by the Home Office Guidelines, which were neither legally binding nor directly publicly accessible. Therefore, the court ruled that the interference with the right to respect for private life was not “in accordance with the law.”

The applicants submitted that obtaining by the police information relating to the numbers called on the telephone in B’s flat constituted an interference with their rights under Article 8 of the Convention. However, the Court noted that the implemented measure was “in accordance with the law.” While it did not appear that there were any specific statutory provisions governing the storage and destruction of such information, the Court was not persuaded that the lack of such detailed formal regulation raised any risk of arbitrariness or misuse. The obtained data did not include any information about the contents of those calls, or who made or received them.

Concerning the use of listening devices in the police station, the Court reiterated that there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life.” Although recordings were made for obtaining voice samples and not for the purpose of using the content of the conversation, a permanent record had nonetheless been made of the person’s voice and it was subject to a process of analysis directly relevant to identifying that person in the context of other personal data. Therefore, recording of the applicants’ voices constituted processing of personal data and interference with the right to respect for private life.

The Court noted that there existed no statutory system to regulate the use of covert listening devices by the police on their premises. No material difference arises where the recording device is operated, without the knowledge or consent of the individual concerned, on police premises. The underlying principle that domestic law should protect against arbitrariness and abuse in the use of covert surveillance techniques applies equally in that situation. The Court concluded that covert recording of a conversation with the aim of obtaining voice samples was not “in accordance with the law.” Therefore, there has been a violation of Article 8 of the Convention.

4.5. AYCAGUER V. FRANCE (2017)

In the case of *Aycaguer v. France*,²¹⁷ the European Court of Human Rights held that due to the duration and the lack of a possibility of deletion, the regulations on the storage of DNA profiles, to which the applicant objected by refusing to undergo sampling, did not provide the data subject with sufficient protection. Therefore, the applicant's conviction for having refused to undergo DNA profiling for inclusion in the database amounted to a disproportionate infringement of his right to respect for private life. There has accordingly been a violation of Article 8 of the Convention.

THE CIRCUMSTANCES OF THE CASE

The applicant attended a rally organized by a trade union, where he struck gendarmes with an umbrella. The applicant was placed in police custody and brought before the Court under the "immediate summary trial" procedure. He was sentenced to two months' imprisonment. Following a request from the Public Prosecutor's Office, the applicant was ordered by the police to give a DNA sample, which he refused. The Court imposed on the applicant a fine and the Court of Appeal upheld that judgment. The Court of Cassation dismissed the applicant's appeal on points of law and noted that the Court of Appeal responded adequately and cogently to the main points of the pleadings submitted to it.

THE COURT'S ASSESSMENT

The Court reiterated that the mere fact of storing data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. At the same time, to protect their population as required, the national authorities can legitimately set up databases as an effective means of helping to punish and prevent certain offences. However, such facilities cannot be implemented as part of an abusive drive to maximise the information stored in them and the length of time for which they are kept.

The applicant had not been included in the FNAEG because he refused to undergo DNA profiling as required by law. He was nonetheless convicted on that basis. It is not contested that that conviction amounted to an interference with the applicant's right to respect for private life. The interference had been in accordance with the law and pursued the legitimate aim of detecting, and therefore preventing, disorder and crime. Therefore, the Court had to examine whether the interference was necessary vis-à-vis the requirements of the Convention.

Since the national authorities make the initial assessment as to where the fair balance lies in a case before a final evaluation by this Court, a certain margin of appreciation is, in principle, accorded by this Court to those authorities as regards that assessment. The breadth of this margin varies and de-

²¹⁷ Available at: <https://bit.ly/3n8wg5K> Date of access: 12.11.2021

depends on several factors, including the nature of the activities restricted and the aims pursued by the restrictions. Where a particularly important aspect of someone's life or identity is in issue, the State's margin of appreciation is generally narrower. Domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of that Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned. The domestic law should, in particular, ensure that such data are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

According to the Code of Criminal Procedure, the duration of storage of DNA could not exceed forty years in the case of persons convicted of offences which the Government considered to display "a specific degree of seriousness". The Court noted that the forty-year period in principle constituted a maximum that should have been adjusted under a separate decree. Since no such decree had ever been issued, the forty-year period was, in practice, treated as indefinite storage, or at least as a norm rather than a maximum.

Only the offences exhaustively listed in the national legislation could give rise to registration in the FNAEG. The Court noted that no differentiation was provided according to the nature and/or seriousness of the offence committed. Events occurring in a political/trade-union context, concerning mere blows with an umbrella directed at gendarmes, contrasted with the seriousness of the acts liable to constitute the very serious offences set out in the legislation, such as terrorism, trafficking, etc. Moreover, access to the deletion procedure was only authorised for suspects, and not for convicted persons. The Court considered that convicted persons should also be given a practical means of lodging a request for the deletion of registered data.

Therefore, the Court considered that owing to its duration and the lack of a possibility of deletion, the regulations on the storage of DNA profiles in the FNAEG, to which the applicant objected by refusing to undergo sampling, did not provide the data subject with sufficient protection. It, therefore, did not strike a fair balance between the competing public and private interests. These facts were sufficient for the Court to find that the respondent State overstepped its margin of appreciation in this sphere. Therefore, the applicant's conviction for having refused to undergo DNA profiling for inclusion in the FNAEG amounted to a disproportionate infringement of his right to respect for private life, and therefore could not be deemed necessary in a democratic society.



5. JUDGMENTS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

This chapter discusses two judgments delivered by the Court of Justice of the European Union relating to the processing of biometric data.

5.1. MICHAEL SCHWARZ V STADT BOCHUM (2013)

The case of *Michael Schwarz v Stadt Bochum*²¹⁸ concerned the processing of fingerprints for the purpose of issuing a passport. The applicant applied to the relevant authority for a passport, but he refused to take part in the mandatory fingerprinting procedure. As a result, his application was rejected. Mr. Schwarz brought an action before the referring court and asked to issue him with a passport without taking his fingerprints. He disputed that the regulation providing rules for fingerprinting did not have an appropriate legal basis, was vitiated by a procedural defect and infringed the rights laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

The Administrative Court referred to the Court of Justice and asked to resolve the issue of the validity of Article 1(2) of Regulation No 2252/2004.

The Court considered that the EU regulation related to the fingerprinting procedure is valid for two reasons: 1) It is adopted on the legal basis - for border control; 2) It serves the purposes of identifying the holder of the document and verifying the authenticity of a passport.

The court noted in the judgment that the fingerprints constitute personal data and the processing of them constitutes a threat to the rights to respect for private life. In this case, it must be ascertained whether such a threat can be justified.

According to the Court's view, another purpose of taking fingerprints is to prevent illegal entry into the European Union and thus genuinely meets an objective of general interest recognised by the Union. It must therefore be ascertained whether this method is necessary for detecting falsifications.

According to the Court's assessment, taking prints of fingers is not an operation of an intimate nature, moreover, it does not cause any particular physical or mental discomfort to the person affected any more than when that person's facial image is taken. Besides, it is an effective way to achieve the goal, as it dramatically reduces the risk of fraud.

The Court noted that the only real alternative to the taking of fingerprints is an iris scan and nothing in the case file submitted to the Court suggests that the latter procedure would interfere less with the rights. Furthermore, fingerprint-recognition technology is more advanced and less expensive than iris-recognition technology. Thus, the first one is more suitable for general use.

The judgment states that the Court has not been made aware of any other measures which would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter.

²¹⁸ Available at: <https://bit.ly/3CfQrTE> Date of access: 13.11.2021.

The court noted that the processing of fingerprints should not go beyond what is necessary to achieve that aim. The legislation must provide specific guarantees that the processing of such data will be effectively protected from misuse and abuse.

In this case, the interference is justified as taking fingerprints constitutes a necessary and proportionate measure to achieve the legitimate aim of protecting against the fraudulent use of passports.

5.2. W. P. WILLEMS AND OTHERS V BURGEMEESTER VAN NUTH AND OTHERS (2015)

In the case of *W. P. Willems and Others v Burgemeester van Nuth and Others*²¹⁹ the Court of Justice of the European Union stated that Regulation (EC) No 2252/2004, with the European Convention on the Protection of Human Rights and Fundamental Freedoms and the Data Protection Directive 95/46 did not provide a legal basis for the Member States not to use the biometric data collected in accordance with the Regulation for purposes other than those provided for in the Convention. The Court clarified that the regulation of the further collection and use of biometric data falls within the competence of the Member States.

Applicants applied to the relevant authority for passports (3 applicants) and identity card (1 applicant). However, their applications were rejected since they had refused to provide digital fingerprints.

The applicants stated in the main proceedings that providing biometric data to the authorized body constituted a serious breach of their right to privacy. The data would be stored on three different media and they might eventually be found on a centralised database of the State. Besides, they did not know who would have access to their personal data.

The first instance did not uphold their claim. This decision was appealed to a higher court, which addressed the following questions to the Court of Justice of the European Union:

1. Must Article 1(3) of Regulation No 2252/2004²²⁰ be interpreted as meaning that it does not apply to identity cards issued by Member States to their nationals, regardless of their period of validity and regardless of the possibilities of using them as travel documents outside the country?
2. Must Article 4(3) of Regulation No 2252/2004,²²¹ Article 8(2) of the European Convention on the

²¹⁹ Available at: <https://bit.ly/3kxqlFV> Date of access: 13.11.2021

²²⁰ Article 1(2) and (3) of Regulation No 2252/2004: Passports and travel documents shall include a storage medium which shall contain a facial image in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. This Regulation applies to passports and travel documents issued by the Member States. It does not apply to identity cards or temporary passports and travel documents having a validity of 12 months or less.

²²¹ According to article 4(3) of Regulation No 2252/2004, biometric data shall be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. For the purpose of this Regulation, the biometric features in passports and travel documents shall only be used for verifying the authenticity of the document or the identity of the holder when the passport or travel document is required to be produced by law.

Protection of Human Rights and Fundamental Freedoms, and Article 7(f) of Directive 95/46 be interpreted as meaning that the Member States should guarantee that the biometric data collected and stored pursuant to that regulation may not be collected, processed and used for any purposes other than the issuing of the document concerned?

Concerning the first question, the Court of Justice of the European Union stated that the regulation does not apply to identity cards and the EU legislature expressly decided to exclude these documents from the scope of that regulation.

As regards the second question, the use and storage of the data are not governed by the Regulation. The regulation does not provide a legal base for setting up or maintaining databases for storage of those data in the Member States and that matter is within the exclusive competence of the Member States.

The regulation does not require the Member States to guarantee, in their legislation, that biometric data collected and stored in accordance with that regulation will not be processed and used for purposes other than the issue of the passport or travel document. This is not a matter which falls within the scope of that regulation. Thus, the court's answer to the second question was negative.



6. SUMMARY

According to European standards, the genetic and biometric data by which a person is uniquely identified belong to special categories of personal data. The processing of such data can simultaneously bring significant benefits and threaten fundamental rights and freedoms. A necessary precondition for their use is the determination of a purpose for which they are collected and processed. Moreover, the data should be processed only to the extent that is necessary to achieve a legitimate aim. Besides, the storage period of personal data should not exceed the time that is necessary to achieve the purpose for which they were collected and processed.

It is of particular importance to implement appropriate technical or organizational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. To ensure data security while creating a new product or service “privacy by design” and “privacy by default” approaches should be adopted.

The use of biometric data and in particular, facial recognition entails heightened risks for data subjects’ rights. Such technologies must be used in accordance with the principles laid down in EU and Council of Europe legislation. Whereas the use of these technologies can be perceived as particularly effective, controllers should, first of all, assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purposes.²²²

As for genetic data, it distinguishes one individual from others, reveals a person’s genetic predisposition to various diseases and health-related information, and determines a person’s ethnic origin and physical characteristics. It should also be noted that it is easy to obtain and extract genetic data from raw materials. At the same time, such data can predict the risk of diseases. What makes them particularly sensitive is the fact that the amount of information that can be obtained from this data is growing with the advancement of technology and research.

To avoid the risks of discrimination, it is important to assess the purpose of genetic data processing. This is how it is possible to determine whether the processing of this data is discriminatory. European legislation pays special attention to the processing of genetic data in the process of employment or insurance, as it is in this context that the greatest risks of discrimination exist. The principles of data protection must be respected during genetic data processing. Often, the processing of genetic data is based on the consent of the data subject. When giving consent, the data subject must be properly informed about the processing objectives and possible risks.

The right to receive information is closely linked to the right of a data subject to refuse to receive genetic information about himself/herself in case he/she wishes so. This right may also apply to family members when, for example, processed data reveals information about a serious illness or unexpected biological links.

²²² Guidelines 3/2019 on processing of personal data through video devices, version 2.0. adopted on 29 January 2020, par. 73, available at <https://bit.ly/3kFg7nN> Date of access: 21.07.2021.



20, T. SHEVCHENKO STREET,
0108, TBILISI, GEORGIA



+ 995 32 292 15 14



INFO@IDFI.GE



WWW.IDFI.GE