



### Informed Consent to Processing of Genetic Data\*

Benedetta Sirgiovanni\*\*

#### Abstract

The paper focuses on the role of informed consent to processing of genetic data in the current and multi-level legal framework.

Firstly, it will seek to determine if it is possible to process genetic data even without any form of consent according to the GDPR. Then, it will show that accountability principle plays a key role not only in the GDPR, but also at international and national levels.

Finally, the paper will point out that nowadays data processing can no longer be regarded as a private relationship between the controller and the data subject. In this context administrative fines imposed by the Data Protection Authority have to be added to the civil liability of the controller. Furthermore, it is recommended to add a preventive remedy like injunctions brought not only by individuals but also by associations, since the approach of data processing is preventive.

#### I. The Role of Consent in the Processing of Special Categories of Personal Data According to EU General Data Protection Regulation 679/2016

Nowadays everyone is aware that if you want to use digital services you have to give your consent to the processing of your personal data.<sup>1</sup> Consent has become nothing more than ticking a box and is one of the steps to access a

\* The paper develops the presentation 'Informed Consent to Processing of Genetic Data' given at the Yufe Law Conference 'Informed Consent', University of Bremen, 27 May 2021.

\*\* Associate Professor of Private Law, Tor Vergata University of Rome.

<sup>1</sup> According to Art 4 (11) GDPR, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. According to Art 7, para 2, 'If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language'. Therefore, the consent is valid if it is informed and specific for that particular matter.

On the rethinking of consent in the data protection framework, see D.J. Solove, 'Introduction: Privacy Self-management and The Consent Dilemma' 126 *Harvard Law Review*, 1883-1888 (2013); A. Mantelero, 'The future of consumer data protection in the E.U. Rethinking the 'notice and consent' paradigm in the new era of predictive analytics' 30 *Computer Law and Security Review*, 643-660 (2014); C. Irti, *Consenso "negoziato" e circolazione dei dati personali* (Torino: Giappichelli, 2021), passim.

service.<sup>2</sup>

After all, consent is not always necessary for the lawfulness of processing of data according to European Union General Data Protection Regulation 679/2016<sup>3</sup> (hereafter GDPR). According to Art 6 of the GDPR<sup>4</sup> consent is only one of the lawful bases for processing data. For example, consent is an alternative option to the pursuit of the legitimate interest of the controller.

What about the processing of special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation? Is consent necessary for the processing of these special categories of personal data?

According to Arts 9(1) and (2)(a) GDPR, processing of special personal data is prohibited unless the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Therefore, consent makes the processing of special data lawful if it is given for specific purposes.

However, if you analyse Art 9 in detail, you will notice that consent is an alternative condition in the processing of special categories of personal data. Art 9(2) states, in fact, that the processing of special categories of personal data is not prohibited if 'processing is necessary for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services (see point h); for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high

<sup>2</sup> According to Recital 32 GDPR, a written statement seeking consent 'could include ticking a box when visiting an internet website'. On the consent as a mechanical matter of 'ticking the box', see E.M.L. Moerel, 'Big data protection. How to Make the Draft EU Regulation on Data Protection Future Proof', 2014, 9, available at <https://tinyurl.com/ym7wea55> (last visited 31 December 2022): '(...) the granting of consent becomes a mechanical matter of 'ticking the box', ie, becomes subject to 'routinisation' and therefore meaningless'.

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at <https://tinyurl.com/yuckr3sk> (last visited 31 December 2022).

<sup>4</sup> Para 1 of Art 6 GDPR states that 'Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.

standards of quality and safety of health care and of medicinal products or medical devices (see point i); for scientific, research or statistical purposes (point j)'.<sup>5</sup>

If one of these conditions is met, it is possible to process special categories of personal data even without any form of consent. So, consent is not the only possible legal basis for data processing, according to Art 9.

## II. The Role of Accountability According to the GDPR

The rationale behind these rules is that the perspective of the protection of personal data has completely changed.<sup>5</sup> All of us are, in fact, aware that it is inevitable that personal data move electronically and physically, and that denying consent to the processing of their personal data means not being able to access a service which is often crucial in modern society. So, the protection of personal data is not based anymore on the ownership of data (where the data subject is the owner of the personal data and can decide to give or to deny consent to the processing of personal data),<sup>6</sup> but on the accountability principle.<sup>7</sup>

Accountability means that the controller has to implement appropriate technical and organisational measures, such as pseudonymisation<sup>8</sup> and data

<sup>5</sup> On the evolution of privacy protection, and, in particular, from the right to be let alone to the right over one's own data, see P. Hummel et al, 'Own Data? Ethical Reflections on Data Ownership' 34 *Philosophy & Technology*, 545 (2021); S. Rodotà, *Il diritto di avere diritti* (Roma-Bari: Laterza, 2012), 396; A.D. Moore, 'Privacy: Its Meaning and Value?' 40 *American Philosophical Quarterly*, 215 (2003); D.J. Solove 'Conceptualizing Privacy' 90 *California Law Review*, 1088 (2002).

<sup>6</sup> On the different opinions about the relationship between personal rights and the ownership right, see S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali* (Milano: Ledizioni, 2018), 53; G. Resta, *Autonomia privata e diritti della personalità* (Napoli: Jovene, 2005), 33; P. Rescigno 'Persona (diritti della)' *Enciclopedia Giuridica* (Roma: Treccani, 1994), XXVI, 3. On the doctrine that criticizes the application of the ownership model to personal rights, see S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, ibidem, 56; D. Messinetti, 'Persona (diritti della)' *Enciclopedia del diritto* (Milano: Giuffrè, 1983), XXIV, 335; O.T. Scozzafava, *I beni e le forme giuridiche di appartenenza* (Milano: Giuffrè, 1982), 543; A. Nicolussi, 'Autonomia privata e diritti della personalità' *Enciclopedia del diritto* (Milano: Giuffrè, 2011), *Annali* IV, 135.

<sup>7</sup> On the accountability principle in the GDPR see, D. Poletti, 'Comprendere il Reg. UE 2016/679: un'introduzione', in A. Mantelero and D. Poletti eds, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa: Pisa University Press, 2018), 15; C. Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello* (Napoli: Editoriale Scientifica, 2018), 89.

On the accountability as a proof of liability, see G. Finocchiaro, 'Introduzione al regolamento europeo sulla protezione dei dati' *Nuove Leggi civili commentate*, 11 (2017). On the accountability as a sign of a paradigm change in the General Data Protection Regulation, see C. Basunti, 'La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali' *Contratto e impresa*, 863 (2020).

<sup>8</sup> Art 4(5) of GDPR states that "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept

minimisation,<sup>9</sup> in order to protect the rights of data subjects.

For this reason, accountability plays a key role in the GDPR (Art 25.1 GDPR): the controller has to account for implementing

‘appropriate technical and organisational measures to ensure a level of security appropriate to the risk, 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’.<sup>10</sup>

In particular, the controller has to ensure that

‘by design and by default, only personal data which are necessary for each specific purpose of the processing are processed (...). In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons’.<sup>11</sup>

In this way the GDPR enhances preventive measures in order to protect data subjects.

### **III. Predictive Ability of Genetic Data and the Prohibition of Discrimination**

According to Art 4(13) GDPR,

“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’.

Genetic data are personal data which are particularly sensitive in relation to fundamental rights. They ‘(...) merit specific protection as the context of their processing could create significant risks to the fundamental rights and

separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person’.

<sup>9</sup> Art 5.1 of GDPR states that ‘Personal data shall be: (...) (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)’.

<sup>10</sup> See J. Alhadeff et al, ‘The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions’, in D. Guagnin et al eds, *Managing Privacy through Accountability* (London: Palgrave Macmillan, 2012), 49-82.

<sup>11</sup> See K. Demetzou, ‘Data Protection Impact Assessment: A tool for accountability and the unclarified concept of ‘high risk’ in the General Data Protection Regulation’ 35 *Computer Law & Security Review*, 6 (2019).

freedoms'.<sup>12</sup> Such data, in fact, not only identify a natural person, but are also able to predict possible future events relating to the person or people biologically close to them. The disclosure of genetic data may inform third parties on any possible future diseases that the data subject and their blood relatives are susceptible to developing throughout life.<sup>13</sup> Therefore, these people could be discriminated against.<sup>14</sup>

For example, insurance companies<sup>15</sup> – as has happened in the United States – may refuse to stipulate insurance contracts for the civil liability of motor vehicles with a person having or possibly developing a genetic disease, or they may decide to stipulate them but ask higher insurance costs, as soon as they become aware of a genetic predisposition of that customer to a neuromuscular disease. This may happen even if the person does not develop that disease or condition, but the person is simply predisposed to it.

Moreover – as observed by the doctrine<sup>16</sup> – genetic information may also influence the choices of an employer. The latter could choose a person who is more genetically resistant to certain environmental working conditions.

We can also imagine that a bank could acquire the information on a possible genetic disease of a specific person and might refuse to conclude a loan contract, or it might decide to conclude it but on condition of the taking out of a credit protection insurance, because it fears the person may not pay all of the loan instalments.<sup>17</sup>

Due to risks of breaching the prohibition of discrimination, the controller has to implement all measures in order to control the flow of genetic data and to

<sup>12</sup> See Recital 51 GDPR, available at <https://tinyurl.com/mr3n8v7e> (last visited 31 December 2022).

<sup>13</sup> On the relationship between genetic information, the individual and the family, see E. Rial-Sebbag, 'Genetic Information: The individual, the family and the Humankind' *Bio Law Journal*, Special Issue, 13 (2021).

<sup>14</sup> On the influence of genetic data on discrimination against a person on the grounds of their genetic heritage, see D. Nelkin, 'Informazione genetica: bioetica e legge' *Rivista Critica del Diritto Privato*, 491-502 (1994), C. Faralli, 'Dati genetici e discriminazione' *Jura Gentium*, 179 (2020).

<sup>15</sup> On the relationship between insurance contracts and genetic data, see S. Barison, 'Assicurazioni «sanitarie» e test genetici in Italia e negli Stati Uniti: affinità materiali e differenze giuridiche fondamentali' *Rivista di diritto civile*, 143 (2000); Y. Joly et al, 'Genetic discrimination in private insurance: global perspectives' 29 *New genetic and society*, 351 (2010), M. Tomasi and C. Casonato, 'Regulating genetic data in insurance and employment: the Italian 'up-stream' way' *Annuario di diritto comparato e di studi legislativi*, 441 (2018).

<sup>16</sup> B. Godard et al, 'Genetic information and testing in insurance and employment: technical, social and ethical issues' 11 *European Journal of Human Genetics*, 129 (2003), M. Simonato and G. Verlenga, 'Law, genes and bioethics: a biomedical perspective' *BioLaw Journal*, Special Issue, 10 (2021).

<sup>17</sup> On data as a new asset class, see K. Birch et al, 'Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech' 1 *Big Data & Society*, 8 (2021) T. Beauvisage and K. Mellet 'Datassets: Assetizing and Marketizing Personal Data', in K. Birch and F. Muniesa eds, *Assetization: Turning Things Into Assets in Technoscientific Capitalism* (Cambridge: MIT Press, 2020), 75-95.

ensure a high level of security to avoid any unauthorised disclosure.<sup>18</sup>

The goal of genetic data protection is to prevent any form of discrimination connected with the use of genetic data by third parties.

#### **IV. International Declaration on Human Genetic Data of 16 October 2003**

International institutions were also aware of risks linked to the processing of genetic data. Therefore, UNESCO adopted the International Declaration on Human Genetic Data on 16 October 2003.<sup>19</sup> As you can read in the preamble to this Declaration, ‘the collection, processing, use and storage of human genetic data have potential risks for the exercise and observance of human rights and fundamental freedoms and respect for human dignity’ and Art 7(a) of this Declaration states that

‘Every effort should be made to ensure that human genetic data (...) are not used for purposes that discriminate in a way that is intended to infringe, or has the effect of infringing human rights, fundamental freedoms or human dignity of an individual or for purposes that lead to the stigmatization of an individual, a family, a group or communities’.

These risks are the consequence of the predictive ability of genetic data.<sup>20</sup>

The genetic data protection in this Declaration is based on informed consent of the collection, and on privacy and confidentiality of processing.

Therefore, on the one hand, a person has to be informed about

‘the purpose for which human genetic data (...) are being derived from biological samples, and are used and stored. This information should indicate, if necessary, risks and consequences. This information should also indicate that the person concerned can withdraw his or her consent, without coercion, and this should entail neither a disadvantage nor a penalty for the person concerned’ (see Art 6(d) of the Declaration).

On the other hand,

<sup>18</sup> On the genetic privacy, see E.W. Clayton et al, ‘The law of genetic privacy: applications, implications, and limitations’ 6 *Journal of Law and Biosciences*, 1 (2019).

<sup>19</sup> Available at <https://tinyurl.com/5bxdsjnv> (last visited 31 December 2022).

<sup>20</sup> As stated in the preamble, genetic data ‘(...) can be predictive of genetic predispositions concerning individuals and that the power of predictability can be stronger than assessed at the time of deriving the data; they may have a significant impact on the family, including offspring, extending over generations, and in some instances on the whole group; they may contain information the significance of which is not necessarily known at the time of the collection of biological samples; (...)’, available at <https://tinyurl.com/5bxdsjnv> (last visited 31 December 2022).

‘Human genetic data, (...) biological samples linked to an identifiable person should not be disclosed or made accessible to third parties, in particular, employers, insurance companies, educational institutions and the family, except for an important public interest reason in cases restrictively provided for by domestic law consistent with the international law of human rights or where the prior, free, informed and express consent of the person concerned has been obtained provided that such consent is in accordance with domestic law and the international law of human rights’ (see Art 14(b) of the Declaration)

and

‘the persons and entities responsible for the processing of human genetic data, (...) and biological samples should take the necessary measures to ensure the accuracy, reliability, quality and security of these data and the processing of biological samples’ (see Art 15).

This International Declaration is soft law; therefore, it is not binding. Rather, it is a model for States to draw upon for their domestic legislation, regulations, ethical codes of conduct and guidelines. Art 1(a) of the Declaration provides that one of the aims of this Declaration is

‘to set out the principles which should guide States in the formulation of their legislation and their policies on these issues; and to form the basis for guidelines of good practices in these areas for the institutions and individuals concerned’.

In other words, States play a key role because they have to implement effectively the provisions laid down by the Declaration.

Art 23(a) of the International Declaration on Human Genetic Data states that

‘States should take all appropriate measures, whether of a legislative, administrative or other character, to give effect to the principles set out in this Declaration, in accordance with the international law of human rights’.

## **V. Decisione Autorità Garante per la Protezione dei Dati Personali 5 June 2019 no 146**

Art 9(4) GDPR states that

‘Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or



data concerning health’.

The European lawmaker considers that the processing of ‘*genetic data, biometric data or data concerning health*’<sup>21</sup> needs a multi-level protection, even though this may compromise the main goal of the EU GDPR, ie, a homogeneous legal system on the processing of personal data in all EU Member States.

The provision in Art 9(4) GDPR has, in fact, to be read taking into account the whole view of the EU GDPR.

On the one hand, the GDPR aims to ensure a consistent and homogenous application of the rules for the processing of personal data throughout the EU, providing a high level of protection to fundamental rights and freedoms of any person. On the other hand, it

‘also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (‘sensitive data’). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful’ (see Recital 10 EU GDPR).

For these reasons Art 21(1) of the decreto legislativo 10 August 2018 no 101<sup>22</sup> (ie the decreto legislativo laying down provisions for the adaptation of national legislation to the provisions of the EU GDPR) has tasked the Italian data protection authority (the ‘Italian DPA’) to adopt an order on sensitive data.

The Italian DPA approved order no 146 on sensitive data on 5 June 2019.<sup>23</sup>

This order contains provisions relating to the processing of genetic data, and in particular relating to the safekeeping and security of genetic data and biological samples.<sup>24</sup>

The aim is to restrict access to these data to identified and authorised people and to use any measures to avoid third parties acquiring these data, even unintentionally. Therefore, this order states that access to a premises must be carried out by a documented procedure established by a document controller. This must include the identification of people who are allowed to access the data in any way out of hours, and such people must be authorised beforehand (para 4.2.a).

Moreover, the transfer of genetic data via electronic messaging systems, including mail, must be carried out using the encryption of data, ensuring the recipient is informed of the cryptographic key by means of communication

<sup>21</sup> On genetic data privacy solutions in the GDPR, see K. Harbord, ‘Genetic data privacy solutions in the GDPR’ 7 *Texas A&M Law Review*, 269 (2019).

<sup>22</sup> Available at <https://tinyurl.com/yx3wxcja> (last visited 31 December 2022).

<sup>23</sup> Available at <https://tinyurl.com/bddz8eae> (last visited 31 December 2022).

<sup>24</sup> See Annex 1 (4.2) of order no 146/2019, available at <https://tinyurl.com/3ta4duw2> (last visited 31 December 2022).

channels other than those used for data transmission (para 4.2.c). The storage of genetic data and biological samples in databases must also be carried out using encryption or pseudonymisation techniques (para 4.2.e).

These techniques make data and samples temporarily unintelligible to any person entitled to access them and allow identification of the data subjects only where necessary, in order to minimise the risks of accidental disclosure or unauthorised or illegal access.<sup>25</sup> The goal is to avoid the identification of the person to whom genetic data or biological samples belong.

The Italian DPA is aware of the role that nowadays control and security play in genetic data protection in order to avoid third parties using these data unlawfully. The order, in fact, starts with specific requirements regarding safekeeping and security. In this context consent is only one step of the processing.<sup>26</sup>

The data subject has to be informed of the purpose of the processing and of the results that can be achieved with the data. The information has to include the unexpected findings that may arise from the processing of genetic data (para 4.3.a).<sup>27</sup> The data controller must give the data subject the chance to limit the scope of genetic data communication and the transfer of biological samples, as well as the possible use of such data for further purposes (para 4.3.b). Thus, the data subject can restrict the movement of their own genetic data.

Nevertheless, it is not laid down that data subject has to be informed of risks and consequences of data communication and of biological samples transfer. For example, the disclosure of data may entail the unlawful use by third parties (such as private companies) and discrimination against the data subject.

Order no 146/2019 entitles the data subject to withdraw consent. In this case processing operations must cease and the data must be erased or made anonymous, including through the destruction of biological samples (para 4.5.1).

<sup>25</sup> On encryption or pseudonymisation techniques, see V. Mayer-Schönberger and Y. Padova, 'Regime change? Enabling big data through Europe's new data protection Regulation' 17 *Science and Technology Law Review*, 328 (2016).

<sup>26</sup> If a data controller changes, the new controller has to provide information to the data subject and acquire new consent. See the Tiziana Life Case, in C. Piciocchi et al eds, 'Legal issues in governing genetic bio banks: the Italian framework as a case study for the implications for citizen's health through public-private initiatives' 9 *Journal of Community Genetics*, 177-190 (2018). Tiziana Life Science is a UK biotechnology company that purchased Shardna, an Italian company, during its bankruptcy proceedings. This Italian company had collected a critical mass of biological samples from 11,700 individuals from ten villages in the mountainous region of Ogliastra in Sardinia in order to identify genes for complex diseases. The aim of Tiziana Life Science was to continue the Shardna project. On 6 October 2016 the Italian Data Protection Authority established the blocking of the processing of the biobank data, and the re-contacting data subjects to provide information and acquire new consent. On 18 May 2017 the Cagliari Tribunal annulled the Italian order. On 7 October 2021, the Supreme Court quashed the decision of the Tribunal. In particular, the Supreme Court stated that the assignment of data causes a new processing. Therefore, the new data controller had to provide information to the data subject and acquire new consent.

<sup>27</sup> On the unexpected findings, see A.O. Cozzi, 'Incidental findings and the right not to know in clinical setting: Constitutional perspectives' *BioLaw Journal, Special Issue*, 106 (2021).

However, the order does not provide that the data subject should be informed of the right of withdrawal of consent and the withdrawal should entail neither a disadvantage nor a penalty for them.

It is true that the Art 13.2(c) GDPR states that

‘the controller shall, at the time when personal data are obtained, provide the data subject with (...) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal’.

Nonetheless, in my opinion, it would be better (*de iure condendo*) not only to introduce a rule providing for the information on risks and consequences of genetic data communication and of biological samples transfer, as laid down by Art 6(d) of the International Declaration on Human Genetic Data, but also the rule in the Italian order providing for the information on the right of withdrawal of consent, as laid down by this Art 6(d) of the International Declaration on Human Genetic Data.

In any case all of us are aware that the withdrawal of consent does not remove genetic data which have already been processed. That is why the withdrawal of consent is not sufficient in order to protect data subjects. It has to be added to all measures aimed at checking genetic data disclosure in order to avoid the unlawful use by third parties.

After all, the Italian DPA lays down requirements for the processing of genetic data without previous consent of the data subject in the case of impossibility of obtaining consent owing to incapacity to act or for natural incapacity. In these cases, the processing may be carried out within the limits of the available genetic data where it is essential for the third party to make an informed reproductive choice or it is justified by the need for the third party to take measures of a preventive or therapeutic nature. If the data subject has died, the processing may also include genetic data extrapolated from the analysis of biological samples of the deceased, provided that it is essential for the third party to make an informed reproductive choice or that it is justified by the need for the third party to take preventive or therapeutic measures (par. 4.7).

Order no 146/2019 also lays down provisions on the processing of genetic data for scientific and statistical research purposes.<sup>28</sup> It is permitted only if it is aimed at protecting the health of data subjects and third parties in the medical, biomedical and epidemiological field. It usually requires the data subjects’ consent; in such cases, the data subjects are required to state whether or not they wish to know the results of the research, including any unexpected news concerning them,<sup>29</sup> if it entails a concrete and direct benefit to them in terms of

<sup>28</sup> See Annex 1 (4.11) of the order no 146/2019, available at <https://tinyurl.com/3ta4duw2> (last visited 31 December 2022).

<sup>29</sup> On the right not to know, see A.O. Cozzi, ‘Incidental findings’ n 27 above, 106.

treatment or prevention or awareness of reproductive choices.<sup>30</sup>

If the data subject withdraws consent to the processing for research purposes, the biological sample must also be destroyed if it has been taken for such purposes, unless the sample cannot be related to an identified or identifiable person by origin or as a result of the processing.<sup>31</sup>

The order provides for further two cases in which consent is not provided. Firstly, genetic data and biological samples of people incapable of giving their consent may be processed for scientific research purposes that do not confer a direct benefit on them. It may be carried out if all of the following conditions are met: (a) the purpose of the research is to improve the health of other people who belong to the same age group or are affected by the same disease or who are under the same conditions as the data subject, and the research programme has received a favourable opinion from the competent ethics committee at local level; (b) research seeking a similar purpose cannot be achieved by processing the data relating to people who can give their consent; (c) consent to the processing is acquired from the lawful guardian, a close relative, a member of the person's family, a cohabitee or, in the absence of them, from the person responsible for the facility where the person concerned is staying; and (d) the research does not entail any significant risks to the dignity, fundamental rights and freedoms of the data subject.<sup>32</sup>

Secondly, it is provided that in the absence of the data subject's consent, biological samples taken and genetic data collected for health protection purposes may be stored and used for scientific or statistical research purposes in the following cases: (a) statistical surveys or scientific research which are required by European Union law, by law or, where so provided for by law, by a regulation; and (b) for the pursuit of further scientific and statistical purposes that are *directly* related to those for which the data subjects' informed consent was originally acquired.<sup>33</sup>

Order no 146/2019 provides that genetic data and biological samples collected for scientific or statistical research purposes may be communicated or transferred to research institutes and organisations, associations and other public and private bodies pursuing research purposes.

This is possible, on condition that it is restricted to information without identifying data, for scientific purposes that are directly linked to those for which the data were originally collected, and as clearly specified in writing in the request for the data and/or samples. In this case, the requesting party must

<sup>30</sup> See Annex 1 (4.11.1) of the order no 146/2019, available <https://tinyurl.com/3ta4duw2> (last visited 31 December 2022).

<sup>31</sup> See Annex 1 (4.11.2) of the order no 146/2019, available at <https://tinyurl.com/yu5arfdb> (last visited 31 December 2022).

<sup>32</sup> *ibid*

<sup>33</sup> See Annex 1 (4.11.3) of the order no 146/2019, available at <https://tinyurl.com/yu5arfdb> (last visited 31 December 2022).

undertake not to process the data and/or use the samples for purposes other than those indicated in the request and not to communicate or further transfer them to a third party.

If you compare the EU GDPR and the Italian Order, it can be concluded that the GDPR is research oriented, whereas in the Italian framework the individual's rights regarding genetic data prevails over the interest of society to benefit from scientific progress.

The GDPR is aware that it is often impossible 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 to certain areas of scientific research, and not to a specific research project.

In fact, Recital 33 GDPR states that

‘Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose’

and Art 5 GDPR lays down that

‘further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’).

In the Italian Order, the data subject can limit the scope of genetic data communication and the transfer of biological samples, as well as the possible use of such data for further purposes. In addition, in the absence of the data subject's consent, biological samples taken and genetic data collected for health protection purposes may be stored and used for scientific or statistical research purposes in for the pursuit of further scientific and statistical purposes that are *directly* related to those for which the data subjects' informed consent was originally acquired.

The connection between further scientific purposes and the purpose for which the data subjects' informed consent was originally acquired is necessary in domestic provisions. The rational under the Italian provisions is to protect the data subject who has the right to control the use of genetic data for specific research taking into account also unexpected findings that may arise from the processing of genetic data. The Italian perspective is that the more you use genetic data the more third parties might be informed of any possible future diseases that the data subject and their blood relatives are susceptible to developing throughout life. Therefore, these people and communities could be discriminated against.<sup>34</sup>

<sup>34</sup> On the relationship between the GDPR and Italian framework in governing genetic

In any case, all provisions (European and domestic Italian provisions) show us that consent is not sufficient, and in some cases, not even necessary, to protect the data subject.

The approach of data processing is preventive: it is based on risk assessment and on prevention measures in accordance with the principle of prevention and with a precautionary principle.<sup>35</sup>

The controller has to take all measures in order to guarantee the non-identification of data subjects to which genetic information refers, keeping the identifying data separate from biological samples and genetic information at the time of collection. Furthermore, the controller has to take all measures to avoid any disclosure of data to third parties that could use them unlawfully, infringing the right of the data subject not to be discriminated against due to their genetic heritage.

In other words, the controller must take every measure to prevent damage, even though the connection between the processing of genetic data and consequential damage is uncertain at the point of collection.

## VI. Algorithms in the Processing of Big Data

The GDPR (and not the Italian Order no 146/2019) contains a provision on automated individual decision-making, including profiling (see Art 22.1). It states that

‘The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’.

In this case the decision-making is based on the processing of data that evaluates personal aspects relating to a person, and in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movement (see Recital 71).<sup>36</sup>

biobanks, see C. Piciocchi et al, ‘Legal issues in governing genetic bio banks: the Italian framework as a case study for the implications for citizen’s health through public-private initiatives’ 9 *Journal of Community Genetics*, 177-190 (2018).

<sup>35</sup> On the difference between the principle of prevention and the principle of precaution, see C. Byk, ‘Precautionary principle and civil law’ 28 *Journal international de bioethique et d’etique des scienses* 35 (2017); A. Trouwborst, ‘Prevention, precaution, logic and law. The relationship between the precautionary principle and the preventative principle in international law and associated questions’ 2 *Erasmus Law Review*, 105 (2009); R. Andorno, ‘The precautionary principle: A new legal standard for a technological age’ 1 *Journal of International Biotechnology Law*, 11 (2004).

<sup>36</sup> ‘The data subject should have the right not to be subject to a decision, which may

Art 22(2) provides that automated decision-making is allowed under some conditions: (a) if it is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) if it is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) if it is based on the data subject's explicit consent.

These exceptions, though, do not apply when the processing is based on special categories of personal data such as genetic data. Automated individual decision-making may cause, in fact, discriminatory effects on people on the basis of genetic status. Algorithms create classes of people through machine learning processes.<sup>37</sup> The selection of genetic data should be avoided because it could generate discriminatory effects against a class of people due to their genetic heritage.<sup>38</sup>

Discrimination against a person on the grounds of their genetic heritage is prohibited in the Italian (and many other) legal system(s). It would infringe the right to dignity and the right to identity guaranteed by Art 2 of the Italian Constitution as inviolable rights of the person.<sup>39</sup>

Furthermore, the prohibition of any form of discrimination against a person on the grounds of his or her genetic heritage is expressly laid down by Art 11 of Oviedo International Convention on Human Rights and Biomedicine adopted on 4 April 1997: 'Any form of discrimination against a person on grounds of his or her genetic heritage is prohibited'.<sup>40</sup> Likewise, Art 6 of the

include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her (...)', available at <https://tinyurl.com/2p8xuy4e> (last visited 31 December 2022).

<sup>37</sup> On the consequence of the use of algorithms in the big data era, see A. Mantelero, 'Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection' 32 *Computer Law & Security Review*, 238 (2016). On risks of profiling, see B.W. Shermer, 'The limits of privacy in automated profiling and data mining' 27 *Computer Law & Security Review*, 45 (2011); K. Wiedemann, 'Profiling and (automated) decision-making under the GDPR: A two-step approach' 45 *Computer Law & Security Review* (2022).

<sup>38</sup> On the risk of big data, see D. Bollier, *The Promise and Peril of Big Data* (Washington: The Aspen Institute, 2010), 25-29; E.M.L. Moerel, *Big data protection* 2 above, 9.

<sup>39</sup> 'The Republic recognises and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed. The Republic expects that the fundamental duties of political, economic and social solidarity be fulfilled', available at <https://tinyurl.com/2acmusvy> (last visited 31 December 2022).

<sup>40</sup> Available at <https://tinyurl.com/2p9b49hs> (last visited 31 December 2022). On Oviedo International Convention on human rights, see R. Andorno, 'The Oviedo Convention: A European legal framework at the intersection of human rights and health law' 2 *Journal of*

Universal Declaration on the Human Genome and Human Rights states that

‘No one shall be subjected to discrimination based on genetic characteristics that is intended to infringe or has the effect of infringing human rights, fundamental freedoms and human dignity’.<sup>41</sup>

The GDPR makes no reference to data aggregation and to the use of algorithms in the processing of genetic data.<sup>42</sup> In my view, it would be better (*de iure condendo*) to add a provision - at least in the order of the Italian DPA – on algorithms applied to the processing of genetic data. In particular, it would be desirable to prohibit explicitly them.

## VII. Private and Public Enforcement

At this point, it is crucial to show what happens if a data controller does not take all appropriate measures with respect to genetic data.

First of all, Art 82.1 of the GDPR states that ‘Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered’. Thus, civil liability of the controller is one of the enforcement regulatory instruments in respect of data protection. This involves compensatory measures for the data subject.

Nevertheless, the European Parliament is aware that data protection has not only an individual dimension, but also a collective one. Data processing – due to the size it has reached in the globalisation era and due to the use of technologies, including algorithms – can no longer be regarded as a private relationship between the controller and the data subject.<sup>43</sup> That is why the public enforcement is necessary. Administrative fines imposed by the Data Protection Authority force the controller to take all appropriate measures to manage risks connected with the processing.<sup>44</sup>

For this reason, Art 21(5) of the decreto legislativo no 101/2018 expressly states that infringements of provisions laid down in the Italian DPA order are

*International Biotechnology Law*, 133 (2005).

<sup>41</sup> Available at <https://tinyurl.com/3v72k7d4> (last visited 31 December 2022).

<sup>42</sup> On data aggregation in data processing, see L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford: Oxford University Press, 2014), 96.

<sup>43</sup> On the change of perspective of data processing, see A. Mantelero, *Personal data* n 37 above, 238, L. Marilotti, ‘I dati genetici tra dimensione individuale e collettiva’ *BioLaw Journal*, 165 (2021).

<sup>44</sup> On the key-role of independent authorities for data processing in the big data era, see A. Mantelero, *Personal data* n 37 above, 245. You will read the following statement ‘(..) independent authorities may play an important role in safeguarding interests related to the collective dimension of privacy and data protection in the big data environment’.



subject to an administrative fine under Art 83(5) GDPR.<sup>45</sup> The latter states that the infringement of the basic principles for processing, including conditions for consent, pursuant to Art 9 on processing of special categories of personal data, including genetic data, are subject to administrative fines of up to € 20 million, or in the case of an undertaking up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.<sup>46</sup>

The pecuniary administrative fine is a very strong incentive for the controller to take all measures to implement GDPR and laws.

### VIII. Conclusions

Informed consent to processing of genetic data is not sufficient (and in some cases, not even necessary) to protect the data subject, according to the GDPR and to the decisione Autorità Garante per la protezione dei dati personali no 146/2019.

The protection of personal data relies on the accountability principle in the current legal system. The controller has to implement appropriate technical and organisational measures, such as pseudonymisation and data minimisation, in order to control the flow of genetic data and to ensure a high level of security to avoid any unauthorised disclosure. In other words, the controller has to take all measures in order to guarantee the non-identification of data subjects to which the genetic information refers, and to avoid any disclosure of data to third parties that may use them unlawfully.

If the genetic data controller does not take every measure to prevent damage, it is liable for damage suffered by any person as a result of this

<sup>45</sup> Available at <https://tinyurl.com/3w23k4zt> (last visited 31 december 2022).

The possibility for national authorities to impose sanctions for cases of infringements is provided for by Art 9, last para, GDPR, which allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data ('Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health'). Available at <https://tinyurl.com/yuckr3sk> (last visited 31 december 2022). Therefore, the Italian DPA order, which establishes infringements, incorporates EU General Data Protection Regulation provisions with regard to genetic data processing.

<sup>46</sup> '5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20000000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Arts 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Arts 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Art 58(2) or failure to provide access in violation of Art 58(1)', available at <https://tinyurl.com/yuckr3sk> (last visited 31 december 2022).

infringement.

Civil liability of the controller is only one of instruments of data protection. The lawmaker, in fact, is aware that civil liability is not a sufficient instrument for the compliance with data protection provisions. Pecuniary administrative fines imposed by the DPA (in short, public enforcement) have to be added to the civil liability of the controller (in short, private enforcement) because they truly force the controller to take all appropriate measures to manage risks connected with processing.

Nevertheless, it should be pointed out that pecuniary administrative fines and civil liability of the controller are both *ex-post* remedies, whereas the approach of data processing is preventive.

Therefore, genetic data subjects, or the group of people biologically close to them, may be interested in intervening immediately in order to prevent any disclosure of genetic data to third parties. That is why it is recommended to expressly include – at least in the order of the Italian DPA – injunctions brought not only by individuals but also by associations as a preventive measure for individual and collective protection of genetic data subjects.<sup>47</sup>

The European Court of Justice is aware that injunctions brought by associations are effective measures in order to prevent infringements of the rights of data subjects to the processing of their personal data.

In fact, in a recent judgment adopted on 28 April 2022, Case C-319/20,<sup>48</sup> the Court ruled that

‘Art 80(2)<sup>49</sup> of the GDPR must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that

<sup>47</sup> See L. Marilotti, *I dati genetici* n 43 above, 165; R. Vecellio Segate, ‘Shifting Privacy Rights from the Individual to the Group: A Re-adaptation of Algorithms Regulation to Address the Gestaltian Configuration of Groups’ 8 *Journal of Regulatory Compliance Loyola University Chicago*, 55 (2022).

<sup>48</sup> Available at <https://tinyurl.com/4z3dkhv2> (last visited 31 December 2022).

<sup>49</sup> Art 80(2) provides that ‘Member States may provide that any body, organisation or association referred to in paragraph 1 of this Art, in- dependently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Art 77 and to exercise the rights referred to in Arts 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing’.

regulation’.

This could be the prelude to a strengthening of injunctions brought by associations in order to prevent any infringements of rights of data subjects including the disclosure of genetic data to third parties.