DIGIPD

WP5 [D5.1; D5.2]

The use of digital biomarkers and machine learning methods in the healthcare sector

GDPR[1] Compliance

Research Centre in Information, Law and Society (CRIDS)
University of Namur

Noémi Bontridder, Researcher at CRIDS, University of Namur
Under the supervision of Cécile de Terwangne, Professor at the Law faculty, University of Namur

July 2022

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Introduction

1. As we are facing a syndemic[2] characterized by, *i.a.*, the aging of the population, research is undergone to improve healthcare services.[3] In this context, special attention is paid to the potential of digital technologies to empower patients and communities to understand their evolving needs. In this line, the main contribution of the DIGIPD project[4] is to assess the extent to which Digital biomarkers (DMs) extracted from voice and face movement recordings as well as mobile gait sensor systems, could help to make an accurate disease diagnosis and treatment-dependent prognosis for each patient.

   When collecting health data through digital devices and using advanced analytical techniques to process these data, special attention must be paid to compliance with the data protection framework. This document reports on the requirements of the General Data Protection Regulation (GDPR) from this perspective.

   First, we will introduce the technological means that are leveraged in the project (1). With a few exceptions,[5] and as long as there is a connecting link with the territory of the European Union,[6] the GDPR applies to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*"[7] As the consortium, acting as controller,[8] is established in the European Union (Belgium, France, Germany, Luxemburg, Spain), processing activities carried out in the framework of the DIGIPD project fall under the territorial scope of the GDPR.[9] We will analyse the different components of the material scope, in order to determine to what extent the GDPR applies to the processing of voice and video recordings, gait signals and the extracted DMs (2). The data protection principles laid down in the Regulation will then be set out and confronted with the processing operations (3), with extended focus on the lawfulness of processing (4-5). Next, the necessary human involvement in the processing operations (6), the obligations of the controller and processor (7) and the rights of the data subjects (8) will be reported.

   A summary applied to the project is included in a box at the end of each section. A conclusion highlights the main obligations of the consortium in the project according to the GDPR.

[2] "*A syndemic is a situation in which two or more interrelated biological factors work together to make a disease or health crisis worse.*" https://www.collinsdictionary.com/submission/23504/syndemic (accessed 28 February 2022).
[3] See European Commission, *Why the EU supports health research and innovation*: https://ec.europa.eu/info/research-and-innovation/research-area/health-research-and-innovation_en (accessed 28 February 2022). On the impact of Covid-19 on health spending in Europe, see the report of the WHO: *Spending on health in Europe: entering a new era*, 2021, available at https://www.euro.who.int/en/publications/abstracts/spending-on-health-in-europe-entering-a-new-era-2021 (accessed 28 February 2022), pp. 61-80.
[4] DIGIPD for "Validating DIGItal biomarkers for better personalized treatment of Parkinson's Disease", http://digipd.eu (accessed 28 February 2022).
[5] See Article 2.2 GDPR.
[6] See Article 3 GDPR.
[7] Article 2.1 GDPR.
[8] See *infra* section 2.3.
[9] Article 3.1 and Recital 22 GDPR.

1. Challenges in personal data protection

1.1. Digital biomarkers: new digital data

2. **Data collection** – As we are living in an advanced technological era, information and communication technologies (ICT) are increasingly pervasive. Computers are present on our desks, we carry mobile phones in our pockets, GPS guide us while travelling, RFID sensors embed our walls, our fridges and bracelets are connected, and our bodies incorporate implants… all generating massive amounts of data, which in turn fuel a range of artificial intelligence applications. At the beginning of 2020, there were 40 times more data found in the digital realm than observable stars in the universe.[10]

3. **The extraction of digital biomarkers in the project** – The project is leveraging the ability of digital tools to collect and process new types of data, as it aims to evaluate the extent to which DMs could contribute to accurate disease diagnosis and treatment-dependent prognosis for each individual patient.

   Following the definition provided by the U.S. National Institutes of Health and the U.S. Food and Drug Administration, a biomarker is "*a defined characteristic that is measured as an indicator of normal biological processes, pathogenic processes, or biological responses to an exposure or intervention, including therapeutic interventions. Biomarkers may include molecular, histologic, radiographic, or physiologic characteristics.*"[11]

   A *digital* biomarker is a new type of medical information that can be used to understand the biological state of the individual like a 'general' biomarker, but its collection is done via digital tools. It can be defined as "*an information – also referred to as 'parameter', 'measure' or technically speaking as 'data' – that is assessed or measured by digital technologies*."[12] In the project, data relating to Parkinson's disease (PD) patients and healthy controls are collected through digital tools in order to extract DMs as follows:

   - Digital biomarkers for speech and voice impairments are extracted from recordings of voice via telephone calls and at the hospital;
   - Digital biomarkers for hypomimia – or reduced facial dynamics – are extracted from video recordings conducted at the hospital;
   - Digital biomarkers for gait impairments are extracted from motion sensors attached to a shoe with a clip and an easy-to-use application on a tablet that guides the instructor through a test set.

   These DMs from sensors and devices allow for a quantitative and continuous monitoring of disease symptoms, also outside clinics. This offers the potential to change fundamentally our understanding of diseases and could help for accurate disease diagnosis and treatment dependent prognosis for each individual patient. This could open the opportunity to adapt medication pathways quickly. In addition, DMs may allow early diagnosis, stratification of patient subgroups and prediction of clinical outcomes.

---

[10] *How Much Data Is Created Every Day? [27 Staggering Stats]*, 28 October 2021, available at https://seedscientific.com/how-much-data-is-created-every-day/ (accessed 19 January 2022).

[11] FDA-NIH Biomarker Working Group, *BEST (Biomarkers, EndpointS, and other Tools) Resource*, 29 November 2021, available at https://www.ncbi.nlm.nih.gov/books/NBK326791/ (accessed 22 January 2022).

[12] H. Fröhlich et al., Leveraging the Potential of Digital Technology for Better Individualized Treatment of Parkinson's Disease. *Frontiers in Neurology*, 28 February 2022, https://doi.org/10.3389/fneur.2022.788427, p. 2.

1.2. Advanced analytical methods

4. **Defining artificial intelligence** – To analyse the multiple data generated by our digital world, the use of AI techniques and methods is particularly appropriate, and even necessary in the presence of vast amounts of data. The term 'artificial intelligence' was given its name by John McCarthy in 1955 when he submitted a funding proposal to the Rockefeller Institute to organise a summer school at Dartmouth. This term refers to a research program: that of reproducing human faculties[13] such as reasoning, calculation, learning, memorization, conceptualization, or decision making, though the use of algorithms.[14] While many have since regretted the choice of name for the field, it persists to this day, and a large number of more or less precise definitions are drafted, including in European documents.

   In 2019, the High-Level Expert Group on AI set up by the European Commission (AI HLEG) adopted the following definition:[15] "*Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).*"

   The Proposal for a regulation contained in the 2020 European Parliament resolution on a framework of ethical aspects of artificial intelligence, robotics, and related technologies[16] defines AI as "*a system that is either software-based or embedded in hardware devices, and that displays intelligent behaviour by, inter alia, collecting, processing, analysing, and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals.*" The French version aptly emphasizes, just like the definition adopted by the AI HLEG cited above, that AI systems rely on data.[17] Pursuant to the proposal,[18] 'autonomy' "*means an AI-system that operates by interpreting certain input and using a set of pre-determined instructions, without being limited to such instructions, despite the system's behaviour being constrained by and targeted at fulfilling the goal it was given and other relevant design choices made by its developer*." This aspect

[13] Marvin L. Minsky, one of the most famous practitioners of the science of AI and cofounder of the Artificial Intelligence Project with John McCarthy, defined AI as "*the science of making machines do things that would require intelligence if done by men.*" M. A. Dennis, "Marvin Minsky". Encyclopedia Britannica, 20 January 2022, https://www.britannica.com/biography/Marvin-Lee-Minsky (accessed 24 January 2022).

[14] D. Lambert, *La robotique et l'intelligence artificielle*, Namur, Editions jésuites, 2019, p. 17.

[15] High-Level Expert Group on Artificial Intelligence (AI HLEG), *A Definition of AI: Main Capabilities and Disciplines*, Brussels, 8 April 2019, p. 6.

[16] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), Article 4 a).

[17] "*«intelligence artificielle», un système qui est soit fondé sur des logiciels, soit intégré dans des dispositifs matériels, et qui fait preuve d'un comportement intelligent, notamment* ***en collectant et traitant des données****, en analysant et en interprétant son environnement et en prenant des mesures, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques*." (emphasis added).

[18] European Parliament resolution on a framework of ethical aspects of artificial intelligence, robotics and related technologies, Article 4 b).

specifically refers to systems developed with machine learning approaches, which rely on statistical inferences and may challenge human oversight.

More recently, the 2021 European Commission proposal for a Regulation on artificial intelligence,[19] defines 'AI system' as a "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.*" This definition reflects a cautionary approach as it refers to an annex that is subject to change. The concerned Annex I distinguishes three types of AI techniques and methods: "*(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods*."[20] AI systems are thus here broadly defined to also encompass traditional expert systems that do not challenge the existing legal framework to the same extent as machine learning methods do. As such machine learning methods rely on statistical correlations, it may be difficult for a human to *understand* why the system reached a specific output, and some algorithms are incomprehensible by design. Yet maintaining human oversight is essential to comply with multiple legal requirements, including those under the GDPR.[21] Research is underway to render deep learning-based systems explainable and understandable.

5. **The use of machine learning methods in the project** – In the project, machine learning methods are used at two stages. First, as digital biomarkers are features extracted from large volumes of collected data about the patients and healthy controls, this extraction is made using machine learning methods. The data collected by the digital devices are signals, and algorithms are applied to these signals to extract the features. The result of the algorithm is a set of abstract features describing some of the patient's characteristics (voice, face movement, gait), which are not necessarily understandable by a human. When such features can be associated to disease symptoms, they can be regarded as candidate DMs. While it is better to make the features understandable, some of the algorithms used are incomprehensible by design. Nevertheless, the current incomprehensibility of the algorithms and features at this first stage does not hamper the understanding of the expected outcomes at the next stage.

   Second, algorithms are sent into the datasets gathering the extracted features to detect subgroups of patients and to cluster multivariate clinical and longitudinal outcome trajectories. In doing this, machine learning methods are used, including unsupervised learning methods. As the aim of the project is to understand which features impact the evolution of the disease, the partners need to

[19] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 24 April 2021, COM(2021) 206 final, Article 3.1.

[20] Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 24 April 2021, COM(2021) 206 final, Annex I.

[21] In particular under the GDPR: transparency and informed consent. Other requirements in the healthcare sector include the fact that only qualified persons are allowed to provide 'healthcare services' and the resulting liability of the physician if things go wrong; and the right of the patient to receive information about his or her health condition and to give informed consent under the Belgian Law on Patient Rights. On these requirements, see W. Buelens, Robots and AI in the healthcare sector: potential existing legal safeguards against a(n) (un)justified fear for 'dehumanisation' of the physician-patient relationship. *Artificial Intelligence and the Law* (eds. J. De Bruyne and C. Vanleenhove), Brussels, Intersentia, 2021, pp. 487-520.

understand what the algorithm does. Undeniably, understanding the outcomes is an integral part of the process. To achieve this, there is no need to understand the features as such.

The project challenges the data protection framework, as the consortium collects new types of data through digital devices and processes these data with advanced analytical methods. Alongside our analysis of the relevant aspects of the GDPR and the corresponding challenges, the following boxes will develop guidelines to be followed to ensure that the project is developed and implemented in compliance with the Regulation.

In the clinical research, the different roles of the partners are summarised as follows for the purposes of this report:
ICM and UKE collect, pseudonymise, organise and store the data. PHCT collects and stores gait signals, on behalf of the consortium (ICM). Amazon Web Services store these gait signals, on behalf of the consortium (ICM). TSP, in turn, analyses the data it accesses through ICM to extract candidate digital biomarkers, and SCAI brings its algorithms to the datasets fed by ICM and TSP, and analyses the statistical results.
UL on its part processes its own algorithms on its own datasets.

2. Key definitions

6. **Foreword** – The GDPR applies to the processing of *personal data*. We will henceforth analyse in this section if voice and video recordings, gait signals and the extracted DMs are to be considered as personal data pursuant to the GDPR. Importantly, we will further analyse if these data enter the special category of health data to which a special regime applies (section 2.1).

   The GDPR applies to the *processing* of personal data, and a special regime is foreseen in the context of scientific research. We will thus hereunder also determine which operations are considered as processing activities and when such processing activities are done for research purposes, according to the GDPR. More precisely, the operations made in the project may be described as profiling operations, a concept used to determine the level of risks at stake (section 2.2).

   Eventually, qualifying the actors as controller or processor in the research project is essential to determine their respective obligations pursuant to the GDPR (section 2.3).

2.1. The data covered

7. **Personal data** – Personal data is defined as "*any information relating to an identified or identifiable natural person*," named the '*data subject*'.[22] Any type[23] of information under any form[24] is thus covered, as long as such information is related to an identified or identifiable natural person (data subject). The GDPR does however not apply to personal data of deceased persons.[25]

   An identifiable natural person is "*one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online*

[22] Article 4.1 GDPR.
[23] The concerned information can either be secret or public, private or relate to professional life, objective or subjective…
[24] It can be for instance a text, a chart, a drawing, an image, a song, biometric or genetic data.
[25] Recital 27 GDPR. Nor are data relating to legal persons covered, as the text refers to natural persons (Recital 14 GDPR).

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[26]

According to this definition, voice recordings, video recordings of face movements, and gait signals are data relating to an identifiable natural person, in this case the patient concerned or the healthy control (data subject). They are therefore personal data as long as the person concerned is alive. The digital biomarkers extracted from these data are personal data as well, as they also relate to the person concerned (data subject).

8. **Sensitive data** – Special categories of personal data, which are referred to as 'sensitive data',[27] are given greater protection because of the increased risks to the data subject that may result from their processing, especially the risks of discrimination.[28] While Article 9 covers the *processing of personal data revealing* characteristics of the data subject considered as sensitive,[29] it also covers the *processing of personal data* considered as sensitive *per se*, irrespective of the purposes of the processing.[30]

9. **Data concerning health** – Among others, '*data concerning health*' are considered sensitive data *per se*. These are defined as "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*."[31] It is further specified that these data "*should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject*."[32]

   A picture of a person may be considered to reveal information about his or her health status when, for example, the person's broken leg is shown. If applied literally, such a picture would be covered by Article 9, irrespective of the purposes of the processing. In this regard, however, the context and purposes of the processing are generally taken into account when classifying health data as sensitive.[33] On the other hand, one could argue that a PD patient's picture or video does not reveal information about this patient's health status *per se*, when only its processing would reveal such information. If applied literally, article 9 would thus not apply in the latter case, and only the digital biomarkers extracted from this personal data would qualify as health data.[34]

---

[26] Article 4.1 GDPR.

[27] Recital 10 GDPR.

[28] Personal data relating to criminal convictions and offences are also given greater protection (Article 10 GDPR).

[29] Namely: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership (Article 9.1 GDPR). The French translation makes it clear that it is the processing itself that reveals sensitive characteristics: « ***Le traitement*** *des données à caractère personnel* ***qui révèle*** *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale* » (emphasis added). This is however questioned by Recital 51, which considers all data mentioned in Article 9 as sensitive data '*by nature*': "*Personal data which are,* ***by their nature****, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin […]"* (emphasis added).

[30] Namely: genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation (Article 9.1 GDPR).

[31] Article 4.15 GDPR.

[32] Recital 35 GDPR.

[33] See J.-M. Van Gyseghem, Les catégories particulières de données à caractère personnel. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, pp. 265-268, n°12.

[34] Following a meticulous analysis of the concept of 'data concerning health' under the data protection framework, such an « objective » interpretation of the GDPR definition was supported by J. Herveg and J.-M. Van Gyseghem in 2018: L'impact du Règlement général sur la protection des données dans le secteur de la santé. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, pp. 722-727, n°22-30. They concluded that "*a strict and objective definition of the concept of health data must be retained, which is limited to*

However, considering the jurisprudence of the European Court of Justice,[35] and as recalled by the EDPB,[36] the term "data concerning health" must be given a wide interpretation. In the context of the COVID-19 outbreak, the EDPB guidelines[37] further indicate that health data can be derived from different sources and cite the following examples:

1) Information collected by a health care provider in a patient record (such as medical history and results of examinations and treatments).
2) Information that becomes health data by cross referencing with other data thus revealing the state of health or health risks (such as the assumption that a person has a higher risk of suffering heart attacks based on the high blood pressure measured over a certain period of time).
3) Information from a "self check" survey, where data subjects answer questions related to their health (such as stating symptoms).
4) Information that becomes health data because of its usage in a specific context (such as information regarding a recent trip to or presence in a region affected with COVID-19 processed by a medical professional to make a diagnosis).[38]

These examples illustrate that some data are health data 'by nature' and other data may become health data because of the purposes and context of their processing. Therefore, we can conclude that any data that is processed to extract digital biomarkers as well as the resulting digital biomarkers are health data that benefit from the protection regime of Article 9 of the GDPR.

10. **Pseudonymised data** – Pseudonymised data is personal data that "*can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept 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.*"[39] Pseudonymised data is considered as information on an identifiable natural person, and is thus covered by the regulation.[40]

    Pseudonymisation is a technique encouraged by the GDPR as its application to personal data "*can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations*."[41]

11. **Anonymous data** – The GDPR does not apply to anonymous information, namely information that "*does not relate to an identified or identifiable natural person,*" nor does it apply to "*personal data rendered anonymous in such a manner that the data subject is no longer identifiable*."[42]

---

information that contains an element of knowledge about the state of health of a (physical) person, thereby excluding any desire to extend the concept to data that do not contain any information about the state of health of a person, even if it is possible to deduce such information (in particular because of the purpose pursued or the context). Indeed, the data that would be inferred or extracted in this way will be automatically protected because of their information content and the data from which they have been inferred or extracted will not be governed by a status that is not appropriate to them [...]." (n°30) (free translation).

[35] Regarding the Directive 95/46/EC, see for instance ECJ, 6 November 2003, C-101/01 (Lindqvist) (judgment) para 50: "*the expression 'data concerning health' […] must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual."*

[36] EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, Adopted on 21 April 2020, p. 5, para 7.

[37] *Ibid.*, p. 5, para 8.

[38] The Article 29 Working Party had also highlighted that "*[p]rofiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.*" Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018, WP260 rev.01 (endorsed by the EDPB during its first plenary meeting – Endorsement 1/2018), p. 15.

[39] Article 4.5 GDPR.

[40] Recital 26 GDPR.

[41] Recital 28 GDPR. See *infra* n° 27.

[42] Recital 26 GDPR.

The GDPR indicates that to determine whether a natural person is identifiable, "*account should be taken of all means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*"[43]

In the healthcare sector, it is rarely possible to anonymize personal data, which are rather pseudonymised. In the present day, personal data is rarely truly anonymized in any sector anyway, given the potential use of AI systems to find back correlations.[44]

The data collected (which include voice recordings, video recordings of face movements, and gait signals) as well as the digital biomarkers extracted from these data, are personal data covered by the GDPR because they relate to identifiable PD patients or healthy controls (who are therefore qualified 'data subjects'). Furthermore, these are sensitive data covered by Article 9 because of the context and purposes of their processing that reveals information about the data subjects' health status. In addition, the digital biomarkers extracted from these data are sensitive data 'by nature'. The fact that the data are pseudonymised is not affecting the GDPR applicability because the concerned patients or healthy controls can still be identified (through additional information kept separately).

2.2. Data processing

12. **Processing** – Processing is defined as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*"[45] Processing is thus broadly described as encompassing any possible operation on data.

13. **Profiling** – Processing of personal data includes profiling, which 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*."[46] Operations made to predict and evaluate the disease trajectories of the patients are therefore profiling operations according to the GDPR.

14. **Processing for the purpose of scientific research** – Even though the term 'scientific research' is not defined in the GDPR, Recital 159 states *that "[f]or the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. […] Scientific research purposes should also include studies conducted in the public interest in the area of public health."* Be that as it may, the EDPB considers that *"the notion may not be stretched beyond its common meaning and*

[43] Recital 26 GDPR.
[44] On anonymised telephone communication data and the possibility of re-identifying data subjects, see the study by Y.-A. de Montjoye et al., On the privacy-conscientious use of mobile phone data. *Scientific Data, No 5*, 11 December 2018, available at https://www.nature.com/articles/sdata2018286.pdf (accessed 17 February 2022).
[45] Article 4.2 GDPR.
[46] Article 4.4 GDPR.

understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice."[47]

Collecting data relating to PD patients and healthy controls already means processing this data, as well as pseudonymizing it, adding it to a catalogue, analysing it using machine learning methods, analysing the results provided by the algorithms and, finally, deleting the data. According to the wording of the definition, any operation on data is indeed considered as data processing within the meaning of the GDPR. In particular, since these operations are carried out to analyse and predict aspects concerning the patients' health, they are described as profiling operations.

Furthermore, all processing activities at stake are carried out by the consortium for scientific research purposes within the meaning of the GDPR.

2.3. The actors

15. **Controller** – The controller is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*"[48] Accordingly, the controller must decide on both the purposes and means of the processing, namely "*the <u>why</u> and <u>how</u> of the processing.* […] *However, some more practical aspects of implementation ("non-essential means") can be left to the processor*."[49] The actual designation of data controllers will be a case-by-case matter as the concept of controller is "*based on a factual rather than a formal analysis.*"[50] As further highlighted by the EDPB, in practice, it is usually the organisation as such, and not an individual within the organisation that acts as a controller.[51]

16. **Processor** – A processor is "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*"[52] Two conditions must be fulfilled to be qualified as processor. First, the processor must be a separate entity in relation to the controller. Second, the processor must process personal data on behalf of the controller. Accordingly, a processor "*is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means*."[53] A processor infringes the GDPR when going beyond the controller's instructions and starting to determine its own purposes and means of processing.[54] In this case, the processor will be considered a controller in respect of that processing.[55]

    When the controller uses cloud computing services, such as Amazon Web Services, the service provider may be qualified as processor depending on the service provided. When using "Infrastructure as a service" cloud computing, the controller only rents computer hardware and does not ask the service provider to process the data on its behalf. The service provider is therefore not a processor. On the other hand, when using "software as a service" cloud computing, the

[47] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 Adopted on 4 May 2020, p. 30, para 153.
[48] Article 4.7 GDPR.
[49] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0 Adopted on 07 July 2021, p. 3.
[50] *Ibid.*, p. 11, para 21.
[51] *Ibid.*, p. 3.
[52] Article 4.8 GDPR.
[53] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (n 49), p. 26, para 80.
[54] Articles 28.10 and 29 GDPR.
[55] Article 29 GDPR.

controller asks the service provider to host its data on its behalf. The service provider is therefore a processor in this case. A third option for the controller is to use "Infrastructure as a platform" cloud computing where the service provider rents not only the hardware but also the operating system. In this case, a case-by-case analysis must be carried out to determine whether the service provider is processing data on behalf of the controller.[56]

17. **Data subject** – The data subject is the natural person who is identified or who can be identified, directly or indirectly by reference to the data that is processed.[57] As J.-M. Van Gyseghem points out, the data subject whose health data is processed, is the patient him/herself and not his/her heirs.[58]

The DIGIPD consortium is the data controller as it decides both the purposes and essential means of the processing of personal data.

PHCT is a processor for the collection of gait signals, which it operates on behalf of the consortium (ICM). Indeed, it is called to implement the instructions given by the consortium with regard to the purpose and means of the collection of gait signals.
Amazon Web Services is a processor as regards the storage of these gait signals, which it operates on behalf of the consortium (ICM). Indeed, it is called to implement the instructions given by the consortium with regard to the purpose and means of the storage of the collected gait signals.

The data subjects are the PD patients and healthy controls whose personal data are processed, because they can be identified by reference to the data processed by the consortium (i.a. voice recordings, video recordings of face movements, gait signals and the extracted digital biomarkers).

3. Principles relating to processing of personal data

18. **Foreword** – The data protection framework is based on six basic principles which must be respected when processing personal data like in the DIGIPD project. These principles are analysed below (sections 3.1 to 3.6).

3.1. Lawfulness, fairness and transparency

19. **Lawfulness** – The first principle recalls that personal data must be processed lawfully,[59] which means that all applicable legal rules must be respected. As one of these legal requirements, the GDPR restrictively lists the circumstances under which processing personal data is permissible in articles 6 to 9.[60]

[56] J. Herveg and J.-M. Van Gyseghem, L'impact du Règlement général sur la protection des données dans le secteur de la santé. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, pp. 731-732, n°35.
[57] Article 4.1 GDPR.
[58] J.-M. Van Gyseghem, Les catégories particulières de données à caractère personnel (n 33), p. 264, n°9.
[59] Article 5.1 (a) GDPR.
[60] Articles 6-9 GDPR and Recital 40. See *infra* section 4.

20. **Fairness** – Personal data must also be processed fairly.[61] As highlighted by the EU institutions, "*[t]he principle of fair processing governs primarily the relationship between the controller and the data subject*."[62] Closely related to transparency requirements, the fairness principle argues for data controllers to inform data subjects and the general public that they will process data lawfully and transparently, and to ensure that data subjects are aware of potential risks. It also obliges controllers to act in a way that promptly complies with the wishes of the data subject, in particular when the data subject's consent is the legal basis for the data processing.[63]

    The fairness principle goes beyond transparency obligations, however, as it relates more generally to the processing of personal data in an ethical manner.[64] In some circumstances, it requires that preference be given to collecting data from data subjects, rather than indirectly from third party sources.[65] This is the case, for example, in the presence of medical data.[66]

21. **Transparency** – Under the transparency principle, personal data must be processed "*in a transparent manner in relation to the data subject.*"[67] Thereon, the GDPR specifies that "*[i]t should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*. […]"[68]

    Accordingly, the controller must take all appropriate measures to provide data subjects with information about how their data is used, in order to empower the data subjects to exercise control over their personal data.[69] As noted by the Article 29 Working Party in its transparency guidelines that were endorsed by the EDPB,[70] the concept of transparency in the GDPR "*is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles.*"[71]

---

[61] Article 5.1 (a) GDPR.

[62] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, *Handbook on European data protection law: 2018 edition*, Luxembourg, Publications Office of the European Union, 2018, https://data.europa.eu/doi/10.2811/58814, p. 118.

[63] *Ibid*., p. 118.

[64] *Ibid*., p. 119.

[65] See C. de Terwangne, Les principes relatifs au traitement des données à caractère personnel et à sa licéité. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, p. 93, n°6.

[66] Council of Europe Committee of Ministers, Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data (adopted 13 February 1997), available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804f0ed0 (accessed 13 February 2022), point 4.2 : "*Medical data shall in principle be obtained from the data subject. They may only be obtained from other sources if in accordance with Principles 4, 6 and 7 of this recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data*."

[67] Article 5.1 (a) GDPR.

[68] Recital 39 GDPR.

[69] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018, WP260 rev.01 (endorsed by the EDPB during its first plenary meeting – Endorsement 1/2018), p.5, para 4.

[70] *Ibid.,* p.5, para 4.

[71] See *infra* section 7.6.

The processing of personal data of PD patients and healthy controls must meet all applicable legal requirements in order to comply with the lawfulness principle of the GDPR. In addition, fairness and transparency are required to empower the data subjects to exercise control over their personal data. This means that the consortium must, *i.a.*, provide the data subject with information about the processing activities carried out, in accordance with its transparency obligations analysed below (section 7.6).

3.2. Purpose limitation

22. **Specified, explicit and legitimate purposes** – According to the purpose limitation principle, personal data must be collected for specified purposes.[72] Hence, these purposes must be specified at the latest at the time of collection of the personal data. The specificity of the purposes is equally necessary not only to enable data subjects to exercise control over their personal data, but also to enable the controller to determine which personal data are necessary for the purposes of the processing[73] and the necessary period of conservation of these personal data.[74] Therefore, a mere reference to the activities of the controller or its legal missions is not sufficient to comply with the purpose limitation principle.[75] Furthermore, still following this principle, the purposes of the processing must be explicit,[76] i.e. they must be announced without ambiguity.[77] Nevertheless, when processing personal data for scientific research purposes, such purposes can be described in more general terms.[78]

    Finally, the purposes must be legitimate.[79] This legitimacy requires that the purposes do not infringe the law and be compatible with the tasks of the controller. It also requires that the purposes pursued through the processing of personal data do not lead to a disproportionate interference with the rights, freedoms and interests at stake. Convention 108+, an instrument of the Council of Europe which contains rules to protect the personal data of individuals similarly to the GDPR,[80] indicates thereon that "*[d]ata processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake*."[81] As noted by C. de Terwangne, "*the interests at stake are, of course, those of the data subject, but also, where applicable, the interests of society as a whole*."[82] Therefore, in the field of medical research, not

[72] Article 5.1 (b) GDPR.
[73] As required under the data minimisation principle. See *infra* n° 24.
[74] As required under the storage limitation principle. See *infra* n° 25.
[75] C. de Terwangne, Les principes relatifs au traitement des données à caractère personnel et à sa licéité. (n 65), p. 95, n°9.
[76] Article 5.1 (b) GDPR.
[77] C. de Terwangne, Les principes relatifs au traitement des données à caractère personnel et à sa licéité. (n 65), p. 95, n°10. This is in line with the transparency requirement provided for in Articles 13.1 (c) and 14.1 (c) GDPR (see *infra* n° 57-58).
[78] Recital 33 GDPR.
[79] Article 5.1 (b) GDPR.
[80] Convention 108+ of the Council of Europe was adopted with reference to the right to privacy enshrined in Article 8.1 of the European Convention on Human Rights. Just like the GDPR, it provides a set of provisions in order to implement the right to protection of personal data.
[81] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Consolidated text, Decision of the Committee of Ministers, 128th Session of the Committee of Ministers, Elsinore, 18 May 2018 (Convention 108+), Article 5.1. The Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) and its Explanatory Report are available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223 (accessed 21 February 2022).
[82] C. de Terwangne, Les principes relatifs au traitement des données à caractère personnel et à sa licéité. (n 65), p. 96, n°11 (free translation). The Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data states in this regard that "*[w]hat is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in*

only the interests of the research team in advancing scientific knowledge must be taken into account but also the interests of society in seeing the possibilities of treatment of the disease under study progress, among others. These interests in the processing of personal data must furthermore be balanced not only with the data subject's right to privacy and data protection, but also, for example, with the collective interest of preserving the capacity for self-determination of the data subjects when continuous monitoring of the disease is envisaged.

Likewise, when techniques for collecting and processing personal data are contemplated in medical practice, the interest of data subjects in benefiting from the most advanced techniques of medical diagnosis and treatment may be balanced with their right to privacy and data protection and the importance of preserving their capacity for self-determination.

23. **Further processing** – The purpose limitation principle prohibits further processing of personal data in a way that is incompatible with the purposes for which they were initially collected.[83] An indicative set of criteria are listed by the Regulation to verify whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, namely: *"(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation*."[84] When compatible with the initial purposes, no lawfulness basis separate from the initial one is required for the envisaged further processing.[85]

Regarding scientific research purposes, the GDPR provides for a "compatibility presumption"[86] provided that appropriate safeguards are implemented in accordance with Article 89.1.[87]

- The purposes of the research project must be specified. In this case, the consortium can indicate that the data will be processed for medical research for better treatment of degenerative diseases (*i.e.*, Parkinson's disease).
- The purposes of the research project must be explicit. The patients must be informed of these purposes (see below section 7.6).
- The purposes must also be legitimate. Considering the latter requirement, we can easily conclude that the scientific research purposes are compatible with the

each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society." (para 48).

[83] Article 5.1 (b) and Recital 50 GDPR. This prohibition is subject to the two following exceptions (Article 6.4 and Recital 50 GDPR): where the processing for a purpose other than that for which the personal data have been collected is based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest as referred to in Article 23(1).

[84] Article 6.4 GDPR.

[85] Recital 50 GDPR: "*The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.* ***In such a case, no legal basis separate from that which allowed the collection of the personal data is required****."* (emphasis added).

[86] This formulation was used by the EDPB in its Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (n 36), p. 10, para 43.

[87] Article 5.1 (b) GDPR: "*further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*." On the appropriate safeguards, see *infra* n° 37.

consortium's tasks. The purposes pursued through each operation on the PD patients' data, which all converge to leveraging the potential of digital biomarkers for better individualized treatment of PD, must also be proportionate in relation to the interference with, *i.a.*, the patients' rights to privacy and data protection. Indeed, there must be a fair balance between, *i.a.*, the interests of society and PD patients to see science progress in this field on the one hand, and the patients' rights to privacy and data protection on the other hand. **The assessment of the proportionality of the processing operations in relation to the purposes** is part of the data protection impact assessment (DPIA) that must be carried out.[88]

Concerning the personal data relating to PD patients that had already been collected before the project, and as long as appropriate safeguards are implemented, the scientific research purposes pursued by the consortium are compatible with the purposes for which the personal data were initially collected. Consequently, no legal basis separate from the one on which the personal data were originally collected is required.
Likewise, the data collected in the project can be further processed for scientific research purposes provided that appropriate safeguards are implemented pursuant to article 89.1 (see *infra* n° 37).

3.3. Data minimisation and storage limitation

24. **Data minimisation** – According to the data minimisation principle, "*personal data shall be […] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*."[89] The latter requirement means that personal data *"should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.*"[90] With respect to a similar provision included in Convention 108+,[91] the Explanatory Report thereto states that *"this requirement not only refers to the quantity, but also to the quality of personal data. Personal data which is adequate and relevant but would entail a disproportionate interference in the fundamental rights and freedoms at stake should be considered as excessive and not be processed.*"[92] The data minimisation principle also requires that the personal data are processed only to the extent necessary to achieve the given purposes.

    The Regulation does not provide for an exception to this principle when personal data are processed for scientific research purposes. The adequacy, relevance and necessity of personal data must therefore be assessed before processing in all cases regarding the purposes pursued. However, as these purposes can be specified in more general terms for the purposes of scientific research,[93] the data that can be processed to achieve these purposes can evolve during the research project. Furthermore, this data minimisation principle does not prohibit research into the adequacy and relevance of specific personal data, such as digital biomarkers, for better treatment of a disease. Indeed, the processing of such biomarkers is necessary to assess their adequacy and

[88] In particular, Article 35.7 (b) GDPR. See *infra* n° 44.
[89] Article 5.1 (c) GDPR. Article 11.1 of the GDPR applies this data minimisation principle by providing that "*[i]f the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*"
[90] Recital 39 GDPR.
[91] Article 5.4 (c) of Convention 108+.
[92] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, p. 9, para 52.
[93] According to Recital 33 GDPR.

relevance for better treatment of the disease. The same conclusion applies to voice recordings, video recordings, and gait signals, as they are adequate, relevant and necessary for the extraction of the digital biomarkers. However, if such personal data are found either inadequate, irrelevant, or unnecessary for the treatment of the disease, their processing would no longer be allowed. The question is always: “is this personal data necessary or not?” If the answer is "no", the personal data cannot be processed.

Precisely if the research concludes that the processing of digital biomarkers allows for a better treatment of the disease, these biomarkers and the personal data from which they are extracted may be processed in medical practice in accordance with the data minimisation principle. Indeed, they could in this case be not only adequate and relevant, but also necessary for the individualized diagnosis and treatment of the disease.

25. **Storage limitation** – Tightly linked with the data minimisation principle, the storage limitation principle requires that “*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 personal data are processed*.”[94] The GDPR specifies that “*[t]his requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. […] In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.*”[95] This means that personal data must be anonymised or erased when they are no longer necessary for the purposes pursued. Therefore, in the research, if digital biomarkers are found either inadequate, irrelevant, or unnecessary for the treatment of the disease, they should be erased. The same applies to voice recordings, video recordings, or gait signals which are no longer relevant for the research. In medical practice, it could be considered that the retention of the patient's personal data is no longer necessary when a certain period has elapsed after remission.[96] This could be the case when the patient has suffered an accident and is completely cured. However, in the case of hereditary diseases, legitimate purposes may justify the retention of the corresponding personal data.

    Insofar as these personal data will be further processed for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes, and provided that appropriate safeguards are implemented,[97] they may be stored for longer periods.[98]

In accordance with the data minimisation principle, voice recordings, video recordings, gait signals, and the extracted digital biomarkers can be processed as long as they are adequate, relevant and necessary for the research purposes pursued. Accordingly, **if such personal data are found either inadequate, irrelevant, or unnecessary for the treatment of Parkinson’s disease, the consortium shall stop their processing and erase them or make them anonymous if the anonymity can be obtained** (see *supra* n° 11). Nevertheless, the consortium may store these personal data beyond this finding, provided that appropriate safeguards are implemented, and solely insofar as they will be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

[94] Article 5.1 (e) GDPR.
[95] Recital 39 GDPR.
[96] See Y. Poullet, *Le RGPD face aux défis de l’intelligence artificielle*, Brussels, Larcier, Coll. du CRIDS 48, 2020, p. 83, n°26.
[97] As required under Article 89.1 GDPR.
[98] Article 5.1 (e) GDPR : *“[…] personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*.”

3.4. Accuracy

26. **Accuracy** – Under the GDPR, personal data must be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*."[99] This obligation of means will be assessed more or less severely depending on the context of the processing.[100] In the medical field, whether in research or in medical practice, it is particularly important that data be accurate because their processing has implications for patients' health. We note that the right of access of data subjects[101] is provided for, among other things, to enable them to identify errors and request their correction.[102] This task of maintaining the accuracy of personal data can be particularly challenging when the data is not "human understandable". This may be the case when features describing characteristics within an individual patient are extracted through machine learning methods.[103]

To comply with the accuracy principle, the consortium must be particularly careful to **maintain the accuracy of the personal data it processes**, how challenging it may be. Indeed, as the features describing characteristics within an individual patient are not human understandable, it may be challenging to maintain their accuracy. Yet, this accuracy is essential in the field of the project (i.e. medical field) as it has implications for the health of PD patients who will benefit from the techniques developed in the project.

3.5. Security

27. **Security of processing** – Personal data must also be processed *"in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*."[104] Accordingly, the GDPR obliges the controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.[105] The GDPR indicates some measures that must be implemented, as appropriate:[106]

    (a) the pseudonymisation and encryption of personal data;
    (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

    Ensuring *confidentiality* of data refers to "*preventing unauthorised access to or use of personal data and the equipment used for the processing*."[107] In this line, the GDPR indicates that the

[99] Article 5.1 (d) GDPR.
[100] As indicated by C. de Terwangne : Les principes relatifs au traitement des données à caractère personnel et à sa licéité. (n 65), p. 111, n°27.
[101] Article 15 GDPR; See *infra* n° 60-61.
[102] The data subjects' right to rectification is provided for in Article 16 of the GDPR; See *infra* n° 62-64.
[103] H. Fröhlich et al., Leveraging the Potential of Digital Technology for Better Individualized Treatment of Parkinson's Disease (n 12), p. 5.
[104] Article 5.1 (f) GDPR. See also Recital 39 GDPR.
[105] Article 32.1 GDPR.
[106] *Ibidem.*
[107] Recital 39 GDPR.

controller and processor must take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.[108]

According to the Article 29 Working Party, *integrity* "*may be defined as the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission. The notion of integrity can be extended to IT systems and requires that the processing of personal data on these systems remains unaltered*."[109]

Measures to ensure a*vailability* and *resilience* of the processing systems are also required, including measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. This testifies the necessity to ensure the continuity of certain processing activities for the protection of privacy of the persons concerned.[110] While ensuring availability of the processing system may not be considered fundamental as regards the processing of personal data for research purposes, it would be crucial in medical practice.[111]

Examples of organizational measures to ensure confidentiality, integrity, availability, and resilience of data are limiting the number of people with access to personal data and using two-factor authentication, as well as protecting physically the infrastructures used to process the personal data. Technical measures may include pseudonymization of data, and the use of a firewall and anti-virus programs.

In assessing the appropriate level of security, the controller and processor must consider the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons.[112] They must especially take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[113] It is specified that "*[t]he likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*"[114]

The GDPR indicates that "*[t]he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage*."[115] An exemplative list of such damages that may stem from personal data processing is provided. In the context of the use of health data for research or medical purposes, the following examples of potential damages stemming from the processing may be particularly relevant: discrimination, loss of confidentiality of personal data protected by

[108] Unless he or she is required to do so by Union or Member State law. Article 32.4 GDPR.
[109] Article 29 Working Party, Opinion 05/2012 on Cloud Computing, Adopted July 1st 2012, WP 196, p. 15.
[110] F. Dumortier, La sécurité des traitements de données, les analyses d'impact et les violations de données. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, p. 154, n°7.
[111] Indeed, the Article 29 Working Party indicated that "*[i]n the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk*." Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018, WP250rev.01 (endorsed by the EDPB during its first plenary meeting – Endorsement 1/2018), p. 9.
[112] Article 32.1 GDPR.
[113] Article 32.2 GDPR.
[114] Recital 76 GDPR.
[115] See Recital 75 GDPR.

professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. Still following the exemplative list, processing of data concerning health may be considered risky, as well as processing where personal aspects are evaluated, in particular analysing or predicting aspects concerning health, in order to create or use personal profiles; where personal data of vulnerable natural persons are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Definitely, the risks[116] stemming from the processing of health data of vulnerable people to predict aspects concerning health require high security measures, and importantly pseudonymisation of the health data that are processed (notably, the additional safeguards mentioned *infra* n° 37).

As stated in the Explanatory Report of Convention 108+, the security measures "*should be kept under review and updated where necessary*."[117]

28. **Notification of a personal data breach to the supervisory authority** – In the case of a personal data breach[118] likely to result in a risk to the rights and freedoms of natural persons, the controller must notify the personal data breach to the competent[119] supervisory authority.[120] The controller must proceed to this notification without undue delay and, where feasible, not later than 72 hours after having become aware of it.[121]

29. **Communication of a personal data breach to the data subject** – In the case of a personal data breach likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject.[122] The controller must proceed to this notification without undue delay.[123] The communication to the data subject is however not required if any of the following conditions are met:[124]

    (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
    (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
    (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

To comply with the security principle as well as security obligations, **high security organisational and technical measures must be implemented by the consortium, PHCT and Amazon Web Services.** These security measures must be high because of the high risks

[116] These are even high risks. See *infra* n° 44.
[117] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, p. 11, para 63.
[118] According to Article 4.12 of the GDPR, "*'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"
[119] In accordance with Article 55 GDPR.
[120] Article 33.1 GDPR. See the subsequent paragraphs of Article 33 for further details regarding the required content of the notification, and other modalities.
[121] Article 33.1 GDPR. "*Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*." Article 33.2 obliges the processor to notify the controller without undue delay after becoming aware of a personal data breach.
[122] Article 34.1 GDPR. See the subsequent paragraphs of Article 34 for further details regarding the required content of the communication.
[123] Article 34.1 GDPR.
[124] Article 34.3 GDPR.

stemming from the processing of health data relating to PD patients, namely vulnerable people.
Organisational measures include limiting the number of people with access to personal data and using two-factor authentication, as well as protecting physically the infrastructures used to process the personal data.
Technical measures include the use of a firewall and anti-virus programs, and pseudonymisation of the patients' data, which is already foreseen. Asking a trusted third party to pseudonymise the personal data is recommended, and even required under the Luxemburg law (see *infra* n° 37).

In case of a personal data breach likely to result in a risk to the rights and freedoms of natural persons, the consortium must notify the personal data breach to the supervisory authority and, where the risk is high, communicate the personal data breach to the data subject.

3.6. Accountability

30. **Accountability** – In accordance with the GDPR, the controller shall be responsible for, and be able to demonstrate compliance with all the principles relating to processing of personal data described above.[125] The general obligation of the controller to be responsible specifies this principle of accountability as follows: "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to **ensure** and to **be able to demonstrate** that processing is performed in accordance with this Regulation*."[126]

    Hence, the controller must implement appropriate and effective[127] measures to ensure that the processing it carries out respects the GDPR. In doing so, it must consider the nature, scope, context and purposes of the processing as well as the risks to the rights and freedoms of natural persons.[128] Furthermore, to be able to demonstrate that the processing respects the GDPR, the controller should document all processing activities and measures adopted, and explain its choices. All measures that are implemented in accordance with this general obligation of responsibility must be reviewed and updated where necessary.[129]

    Many of the controller's obligations[130] implement this principle of accountability through concrete measures, such as the obligation to carry out a data protection impact assessment[131] and the obligation to maintain a record of processing activities.[132]

In accordance with the accountability principle, the consortium is responsible for complying with the GDPR and must be able to demonstrate this compliance. Therefore, **the consortium should document all processing activities and the measures implemented to comply with the Regulation.**

[125] Article 5.2 GDPR.
[126] Article 24.1 GDPR (emphasis added).
[127] Recital 74 GDPR.
[128] Recital 75 of the GDPR lists risks to the rights and freedoms of natural persons.
[129] Article 24.1 GDPR.
[130] See *infra*, section 7.
[131] Article 35 GDPR. See *infra* n° 44.
[132] Article 30 GDPR. See *infra* n° 53.

4. Lawfulness of processing

31. **Foreword** – The GDPR restrictively lists the circumstances under which personal data can be lawfully processed. We will therefore hereunder analyse the potential lawful bases for the processing activities carried out in the project (sections 4.1 to 4.3).

32. **Derogation regime** – In view of the risks generated by the processing of sensitive data, such as health data, for the data subject, such operations are generally prohibited by the GDPR,[133] but exceptionally allowed in certain limited circumstances.[134] These circumstances must be interpreted restrictively[135] in the interest of the data subject.

    As we have seen (*supra* n° 23), the further processing of existing datasets for research purposes is compatible with the purposes for which they were collected. Hence, no legal basis distinct from the initial one is required in this case, provided that appropriate safeguards are implemented.[136]

4.1. Explicit consent

33. **Derogation based on explicit consent** – There is a lawful basis for processing sensitive data, including health data, where the data subject "*has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition [to process sensitive data] may not be lifted by the data subject*."[137] This consent must not only be explicit[138] but also freely given, specific, informed, unambiguous, and made by way of a statement or 'clear affirmative action'.[139]

    In the context of scientific research, the EDPB aptly emphasises that "[w]*hen consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard*."[140]

34. **Consent must be freely given** – The EDPB considers that "*[t]he element "free" implies real choice and control for data subjects*. *As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid*."[141] The GDPR specifies also that "*consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller* […]."[142] In this regard, the EDPB highlights that "*this will be the case when a participant is not in good health conditions, when participants belong to an economically or socially disadvantaged group or in any situation of institutional or hierarchical*

[133] Article 9.1 GDPR.
[134] Article 9.2 GDPR.
[135] Like any other exception.
[136] In accordance with Article 89.1 GDPR.
[137] Article 6.1 (a) combined with Article 9.2 (a) GDPR.
[138] Article 9.2 (a) GDPR.
[139] Article 4.11 GDPR.
[140] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 (n 47), p. 30, para 154. See also Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) Adopted on 23 January 2019, pp. 5-6, paras 15-16.
[141] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 (n 47), p. 7, para 13.
[142] Recital 43 GDPR.

dependency."[143] There may for instance be such an imbalance in the case of clinical trials on the elderly or on a person who does not have access to treatment and for whom the clinical trial may be the only potential cure.[144]

Consent may thus not be an appropriate lawful basis for the processing of health data for medical research purposes. The same conclusion applies in medical practice, as the patients may endure negative consequences if they do not consent to the processing of their health data.

35. **Consent can be withdrawn** – Moreover, consent can be withdrawn by the data subject at any moment.[145] While such withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal, it could consistently affect the research undergone where successive processing of the data is required. In this regard, the EDPB "*notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there is no exemption to this requirement for scientific research."*[146] It is important to note that the controller cannot swap from consent to other lawful bases.[147] It is therefore not allowed to retrospectively utilise the scientific research purposes lawful basis in order to justify processing, where problems have been encountered with the validity of consent. Indeed, "[b]*ecause of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is*."[148]

    The EDPB further adds that "[i[*f a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research*."[149] Such an interpretation however eludes the fact that, following the text of the GDPR, withdrawal of consent does not oblige by itself the controller to erase the personal data[150] and that the right to erasure[151] may be restricted where the processing is necessary for achieving scientific research purposes.[152]

Consent as a lawful basis for processing personal data under the GDPR must be distinguished from other consent requirements that serve as an ethical standard or procedural obligation.
Importantly, while the consent of healthy controls is a lawful basis for the processing of their personal data, the PD patients' consent may not be a lawful basis for processing their health data because such consent is not freely given as requested under the GDPR: there may be a lack of balance between the consortium and the PD patients (vulnerable / elderly persons) in the research project (clinical trial). Therefore, it would be more appropriate to base the processing operation on another lawful basis (*i.e.*, scientific research purposes).

[143] Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)) (n 140), p. 6, para 20.
[144] Th. Léonard and O. Guerguinov, Dérogations au RGPD applicables à la recherche scientifique en Belgique. *Revue du droit des technologies de l'information n°76-77*, août 2020, p. 24, n°17.
[145] Article 7.3 GDPR.
[146] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 (n 47), p. 32, para 164.
[147] *Ibid*., p. 25, para 123.
[148] *Ibid*., p. 25, para 123.
[149] *Ibid*., p. 32, para 164.
[150] Th. Tombal, Les droits de la personne concernée. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, p. 464, n°77; see also Th. Léonard and O. Guerguinov, Dérogations au RGPD applicables à la recherche scientifique en Belgique (n 144), pp. 26-27, n°19.
[151] Article 17 GDPR. See *infra* n° 65.
[152] Article 17.3 (d) GDPR. See *infra* n° 67.

4.2. Scientific research

36. **Derogation based on research purposes** – The GDPR foresees a specific derogation to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for the purposes of scientific research[153] "*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*."[154]

    Following the text, this derogation must be based on a specific legislation.[155] While the Luxemburg law provides for such a derogation in application of this provision,[156] it is not the case of the Belgian law. If applied literally, and in the absence of a specific Union legislation, processing sensitive data for research purposes could only be carried out based on the data subject's explicit consent when the national legislation does not foresee such derogation. Th. Léonard and O. Guerguinov[157] however consider that the text is not coherent and should be interpreted in favour of the general interest and the rights and freedoms of people concerned. On this basis, they conclude that it should be possible to process sensitive data where necessary for scientific research purposes, even in the absence of a specific Union or national legislation.

37. **Additional safeguards in the context of scientific research** – Appropriate safeguards for the rights and freedoms of the data subject are specifically required when personal data are processed for the purposes of scientific research, including pseudonymisation provided that the purposes can be fulfilled in that manner.[158]

    While in this regard the provision specifically refers to the GDPR, seeming to exclude the intervention of the national and European legislators,[159] the Luxemburg law interestingly specifies the required measures.[160]

---

[153] Article 6.1 (f) combined with Article 9.2 (j) GDPR.

[154] Article 9.2 (j) GDPR.

[155] Which must, *inter alia*, provide for suitable and specific measures to safeguard the fundamental rights of the data subject. Such measures are however already required under Article 89.1 of the GDPR.

[156] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Articles 64 and 65. On the measures that must be implemented pursuant to Article 65, see note 160.

[157] Th. Léonard and O. Guerguinov, Dérogations au RGPD applicables à la recherche scientifique en Belgique (n 144), p. 32, n°25.

[158] Article 89.1 GDPR: "*Processing for achieving […] scientific […] research purposes […], shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner*."

[159] Th. Léonard and O. Guerguinov, Dérogations au RGPD applicables à la recherche scientifique en Belgique (n 144), p. 31, n°25.

[160] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Article 65: "*Taking into account the nature, scope, context and purposes of the processing and the risks to the rights*

The fact that processing PD patients' and healthy controls' health data is necessary to achieve scientific research purposes constitutes a lawful basis for their processing, **provided that appropriate safeguards are implemented pursuant to article 89.1.**

4.3. Preventive or occupational medicine, medical diagnosis

38. **Derogation based on medical purposes** – Processing health data is also permissible where it "*is necessary for the purposes of preventive or occupational medicine, […] medical diagnosis, the provision of health or social care or treatment […] on the basis of Union or Member State law or pursuant to contract with a health professional […]*."[161] In this case, those data must be processed "*by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies*."[162]

If the research results are conclusive, digital biomarkers and the personal data from which they are extracted could be processed in medical practice by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person subject to an obligation of secrecy.

5. Additional conditions for processing health data

39. **Additional conditions under national laws** – In addition to all requirements under the GDPR, Member States are entitled to "*maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health*."[163]

and freedoms of natural persons, the controller of a processing operation carried out for scientific or historical research purposes, or for statistical purposes, must implement the following additional appropriate measures:
1° the appointment of a data protection officer;
2° carrying out an analysis of the impact of the planned processing operations on the protection of personal data;
3° anonymisation, pseudonymisation within the meaning of Article 4.5 of Regulation (EU) 2016/679 or other functional separation measures ensuring that data collected for scientific or historical research purposes, or for statistical purposes, cannot be used to take decisions or actions in relation to the data subjects;
4° the use of a trusted third party functionally independent of the controller for the anonymisation or pseudonymisation of data;
5° encryption of personal data in transit and at rest, as well as state-of-the-art key management;
6° the use of technologies that reinforce the protection of the privacy of the persons concerned;
7° the implementation of restrictions on access to personal data within the controller;
8° log files that make it possible to establish the reason, date and time of the consultation and the identification of the person who collected, modified or deleted the personal data;
9° awareness-raising among staff involved in the processing of personal data and professional secrecy;
10° regular evaluation of the effectiveness of the technical and organisational measures put in place through an independent audit;
11° the prior establishment of a data management plan;
12° the adoption of sectoral codes of conduct as provided for in Article 40 of Regulation (EU) 2016/679 approved by the European Commission pursuant to Article 40.9 of Regulation (EU) 2016/679.
The controller must document and justify for each project for scientific or historical research or statistical purposes the exclusion, if any, of one or more of the measures listed in this Article." (Free translation).

[161] Article 6.1 (f) combined with Article 9.2 (h) GDPR.

[162] Article 9.3 GDPR.

[163] Article 9.4 GDPR.

While, in application of this provision, the Belgian law imposes on the controller to implement three additional measures when genetic, biometric or health data are processed,[164] the Luxemburg law only prohibits the processing of genetic data for the purpose of exercising the data controller's own rights in relation to employment law and insurance.[165]

When processing health data of PD patients, the consortium should pay attention to **potential additional conditions foreseen by applicable national laws.**

6. Prohibition on solely automated individual decision-making

40. A data subjects' right – As a preliminary remark, we note that the general prohibition on solely automated individual decision-making with legal or similarly significant effects, is included in the GDPR chapter on the data subjects' rights.[166] We have deliberately chosen to highlight this prohibition because it is binding on the controller, regardless of any action taken by the data subject.[167]

41. Right not to be subject to automated individual decision – The data subject "*has 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*."[168] A Recital of the GDPR explicitly specifies that "*[s]uch 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 […] health, […] where it produces legal effects concerning him or her or similarly significantly affects him or her*."[169]

[164] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Article 9 : *« Pursuant to Article 9.4 of the Regulation, the controller shall take the following additional measures when processing genetic data, biometric data or data concerning health:*

1° the categories of persons having access to the personal data, are designated by the controller or, where applicable, by the processor, with a precise description of their function in relation to the processing of the data concerned;

2° the list of the categories of persons thus designated is kept at the disposal of the competent control authority by the controller or, where applicable, by the processor;

3° it ensures that the designated persons are bound by a legal or statutory obligation, or by an equivalent contractual provision, to respect the confidentiality of the data concerned." (free translation).

[165] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Article 66.

[166] Namely, Chapter III of the GDPR.

[167] This was also highlighted by the Article 29 Working Party in its Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (n 38), pp. 19-20: "*The term "right" in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data*. […] *Interpreting Article 22 as a prohibition rather than a right to be invoked means that individuals are automatically protected from the potential effects this type of processing may have. The wording of the Article suggests that this is the intention and is supported by Recital 71*."

[168] Article 22.1 GDPR.

[169] Recital 71 GDPR.

The GDPR foresees several exceptions to this right,[170] but none of them applies where the processing is based on research purposes[171] or on medical purposes[172].[173]

Regarding the impactful effects of the decision covered by the prohibition, the Article 29 Working Party specifies that "[f]*or data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:*

- *significantly affect the circumstances, behaviour or choices of the individuals concerned;*
- *have a prolonged or permanent impact on the data subject; or*
- *at its most extreme, lead to the exclusion or discrimination of individuals*."[174]

Diagnosis and treatment decisions have sufficiently significant effects on the data subject to meet the threshold because they have a prolonged or permanent impact on the data subject. Therefore, processing health data, including digital biomarkers, through machine learning methods cannot lead to a diagnosis or treatment decision based solely on automated decision-making.

42. **The necessity of human involvement** – The prohibition refers to decisions '*solely based*' on automated processing. According to the Article 29 Working Party, this means that there is no human involvement in the decision process. It illustrates this by stating that "[a]*n automated process produces what is in effect a recommendation concerning a data subject. If a human being reviews and takes account of other factors in making the final decision, that decision would not be 'based solely' on automated processing*."[175] It also indicates that "[t]*o qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data*."[176]

The Recommendation of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Council of Europe) gives guidelines where decisions are taken using technological systems:[177]

> 5.6 […] when the profiling system issues a decision or a draft decision, it is strongly recommended that:
> a. the controller considers all the particularities of the data and does not simply rely on information or processing results taken out of context;
> b. in the event of high-risk profiling, the controller informs the data subject of the algorithmic operations underlying the data processing, including the consequences of these operations for him or her. The information should be such as to enable the data subject to understand the justification for the decisions or draft decisions;
> c. the person appointed by the controller is able, on the basis of reasonable arguments, to decide not to rely on the results of the recommendations arising from the use of profiling;
> d. where there are indications of direct or indirect discrimination based on the functioning of the profiling operation, controllers and processors provide evidence of the absence of discrimination.

---

[170] See Article 22.2-4 GDPR.
[171] Pursuant to Article 6.1 (f) combined with Article 9.2 (j) GDPR. See *supra* n° 36.
[172] Pursuant to Article 6.1 (f) combined with Article 9.2 (h) GDPR. See *supra* n° 38.
[173] See Article 22.4 GDPR.
[174] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (n 38), p. 21.
[175] *Ibid.*, p. 20.
[176] *Ibid.*, p. 21.
[177] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 3 November 2021, available at https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46147 (accessed 30 January 2022).

5.7. Persons affected by a decision based on profiling should have the right to receive a meaningful explanation of this decision or draft decision to understand the justification for it. Intellectual property or the existence of trade secrets may only be opposed where the information to be given would seriously affect these rights. The invocation of these rights and interests by the controller may not lead to deprive the data subject or the affected group of the capacity to understand the decisions or draft decisions taken by the controller.

5.8. Notwithstanding recourse before a supervisory authority or legal redress, data subjects should have the right to challenge the profiling before a person nominated by the data controller, who has access to all the information about the profiling and its functioning, and is qualified to modify or delete the decision or draft decision.

As highlighted by W. Buelens,[178] "*whether the physician's decision is based solely on automated processing in the sense of Article 22(1) GDPR depends on the factual circumstances. Thus, if a physician's intervention is de facto limited to nominal oversight and the results are automatically/routinely applied to individuals without any actual influence on the result ('rubber-stamping') – which may be justified depending on the patient's health condition and the risks involved – the decision may be qualified as based 'solely' on automated processing of personal (health) data in the sense of Article 22(1) GDPR.*"

The fact that decisions of physicians cannot be based solely on an automated processing of personal data also stems from the fact that only qualified persons are allowed to provide healthcare.[179]

Understanding the outcomes of the processing operations must stay the primary aim of the research, as digital biomarkers and the advanced analytical methods will not be usable in medical practice if a human cannot take decisions based on the outcomes.
Accordingly, the consortium must ensure that the algorithms used to predict the evolution of the disease of patients and to cluster subgroups of patients are understandable and therefore do not preclude the physicians to take the decisions, even if the features are not understandable as such.

7. Obligations of the controller[180] and processor

43. **Foreword** – In addition to the basic principles analysed above (section 3) that must be respected all along the project, the GDPR prescribes specific obligations incumbent upon the controller and/or upon both the controller and processor who process personal data such as in the DIGIPD project. We highlight and analyse these obligations hereunder (sections 7.1 to 7.6).

7.1. Data protection impact assessment (obligations of the controller)

44. **Data protection impact assessment** – Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller must carry out a "*data protection impact assessment*" prior to the processing.[181] A single assessment can address "*a set of similar processing*

[178] W. Buelens, Robots and AI in the healthcare sector: potential existing legal safeguards against a(n) (un)justified fear for 'dehumanisation' of the physician-patient relationship. (n 21), pp. 514-515, n°30.
[179] See *Ibid.*, pp. 493-494, n°6-7.
[180] The principle of accountability generates crucial general obligations for the controller. On this principle and the related obligations, see *supra* n° 30.
[181] Article 35.1 GDPR.

operations that present similar risks."[182] The GDPR specifies that such assessment is required in particular where the processing is leveraging new technologies,[183] and where processing leads to "*a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*" or in the case of "*processing on a large scale of special categories of data [including data concerning health] […]*."[184]

The Article 29 Working Party has provided a list of nine criteria to guide the national supervisory authorities which must "*establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment* […]."[185] This list includes four criteria of relevance regarding the potential use of digital biomarkers in the healthcare sector:[186]

- Automated decision-making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" […].[187]
- Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 […].
- Data concerning vulnerable data subjects: the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children […], more vulnerable segments of the population requiring special protection (mentally ill persons, […] *the elderly, patients*, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
- Innovative use or applying new technological or organisational solutions […]. The GDPR makes it clear[188] that the use of a new technology, defined in "*accordance with the achieved state of technological knowledge*"[189], can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

The assessment shall contain at least:[190]

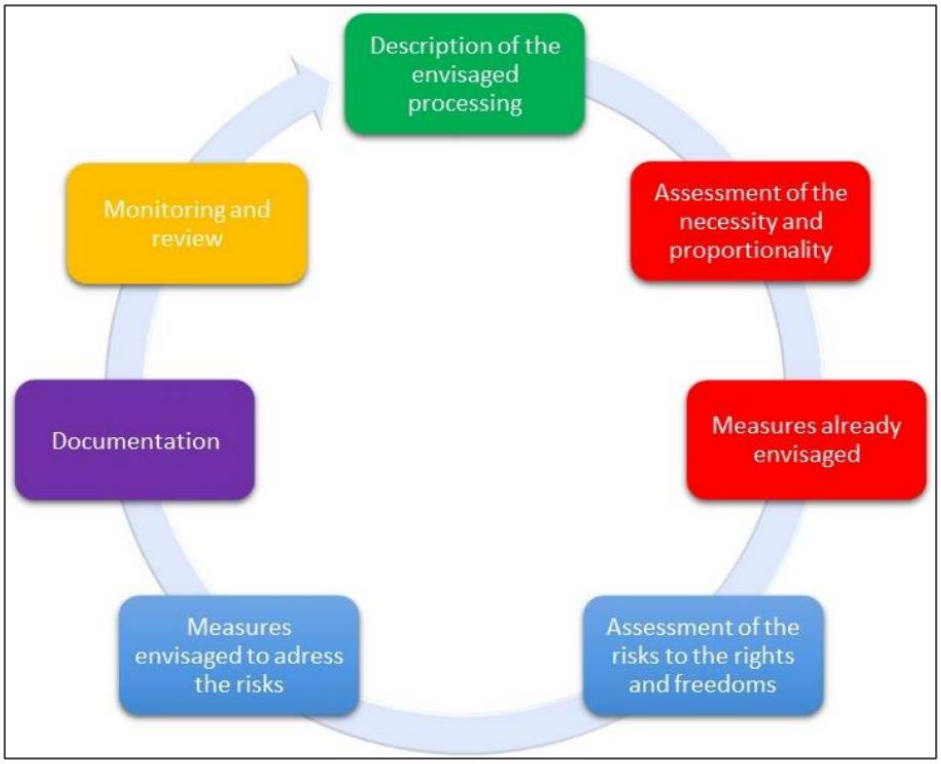
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects […]; and
(d) the measures envisaged to
    - address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data

[182] *Ibidem.*
[183] *Ibidem.*
[184] Article 35.3 (a) and (b) GDPR.
[185] Article 35.4 GDPR.
[186] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, WP 248 rev.01, pp. 9-10 (emphasis added).
[187] In accordance with Article 35.3 GDPR.
[188] (Article 35(1) and recitals 89 and 91).
[189] (Recital 91).
[190] Article 35.7 GDPR.

- demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

It is specified that where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing.[191] This measure is especially appropriate in the context of medical research, and it is an integral part of the DIGIPD project to collect and analyse the views of PD patients regarding the use of sensitive data for better treatment of their disease.[192]

The following figure illustrates the generic iterative process for carrying out a DPIA:



© Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p. 16

The consortium, PHCT and Amazon Web Services shall carry out a data protection impact assessment (DPIA) because sensitive data (health data) concerning vulnerable persons (PD patients / elderly) are processed in the project.

This DPIA, carried out in an iterative process, shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued by the consortium (scientific research purposes);
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects […]; and
(d) the measures envisaged to
   - address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data (including pseudonymisation).
   - demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

[191] Article 35.9 GDPR.
[192] See http://digipd.eu (accessed 28 February 2022).

7.2. Designation of a data protection officer

45. **Designation of a DPO** – The controller and the processor processing, on a large scale, health data such as digital biomarkers and the personal data from which they are extracted, are required to appoint a "*data protection officer*" (DPO), either internal or external to the organisation, with professional qualities and knowledge of data protection law and practice.[193]

46. **Position of the DPO** – The status of the DPO should be such as to ensure direct access to the highest level of management, independence and impunity in the performance of his or her duties. (S)he shall be involved by the controller and the processor in all issues which relate to the protection of personal data.[194] (S)he shall carry out any task within the company in order to inform, advise and ensure compliance of processing operations with data protection legislation.[195]

The consortium as well as PHCT and Amazon Web Services must appoint a Data Protection Officer (DPO) because they process health data on a large scale. This DPO must be designated on the basis of professional qualities and expert knowledge of data protection law and practices and the ability to fulfil the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b) to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.[196]

The consortium, PHCT and Amazon Web Services must provide the DPO with direct access to the highest level of management, independence and impunity in the performance of his/her duties. They must involve the DPO in all issues relating to the protection of personal data.

7.3. Data protection by design and by default (obligations of the controller)

47. **Data protection by design** – In accordance with its general responsibility to ensure that processing is performed in accordance with the GDPR,[197] the controller shall "*both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures […], which are designed to implement data-protection principles […], in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data*

[193] See Article 37 GDPR.
[194] See Article 38 GDPR.
[195] See Article 39 GDPR. On the role, status and prerogatives of the DPO, see K. Rosier, Délégué à la protection des données : une fonction multifacette. *Le règlement général sur la protection des données (RGPD/GDPR)* (eds. C. de Terwangne and K. Rosier), Brussels, Larcier, Coll. du CRIDS 44, 2018, pp. 559-592.
[196] Article 39 GDPR.
[197] See *supra* n° 30.

subjects."[198] The measures could consist of, *i.a.*, "*minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.*"[199] In order to evaluate the appropriate measures, the controller must consider the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons.[200]

48. **Data protection by default** – In accordance with its general responsibility to ensure that processing is performed in accordance with the GDPR,[201] the controller shall also "*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.*"[202] The principle of data protection by default especially obliges the controller to operationalize the principles of data minimisation[203] and storage limitation.[204] Hence, it is included in the principle of data protection by design.[205]

Appropriate technical and organisational measures must be implemented by the consortium to respect the data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
These measures are the ones specified in sections 3.1 to 3.5. Attention must be paid to their respect all along the research project.

7.4. Relation between controller and processor

49. **The controller must choose the right processor** – The controller who is considering using a processor, must verify that the latter provides "*sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*."[206] The sufficient guarantees must be provided "*in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing*."[207]

50. **The obligation to conclude a contract** – The GDPR foresees that processing by a processor "*shall be governed by a contract or other legal act under Union or Member State law, that is binding on*

[198] Article 25.1 GDPR.
[199] Recital 78 GDPR.
[200] Article 25.1 GDPR.
[201] See *supra* n° 30.
[202] Article 25.2 GDPR.
[203] See *supra* n° 24.
[204] See *supra* n° 25.
[205] It however clarifies that "*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*." (Article 25.2 GDPR).
[206] Article 28.1 GDPR.
[207] Recital 81 GDPR. "*The adherence of the processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element to demonstrate sufficient guarantees […]*." (Article 28.5 GDPR).

the processor with regard to the controller."[208] This contract (or other legal act) shall be in writing, including in electronic form.[209]

Taking into account the risk to the rights and freedoms of the data subject,[210] the contract must set out *"the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller*."[211] The contract must also indicate a series of obligations incumbent upon the processor, namely that it:[212]

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32;[213]
(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;[214]
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;[215]
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;[216]
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.[217]

51. **Cascading subcontracting** – Where the initial processor wishes to engage another processor to carry out specific processing activities on behalf of the controller, it must have received prior written authorisation of the controller to do so.[218] This authorisation can be specific or general. In the latter case, the initial processor must inform the controller "*of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.*"[219]

Where the initial processor engages another processor, a contract (or other legal act) must impose on this other processor the same obligations as the ones set out in the contract between the controller and the initial processor, so that the processing will meet the requirements of the

[208] Article 28.3 GDPR.
[209] Article 28.9 GDPR.
[210] Recital 81 GDPR.
[211] Article 28.3 GDPR.
[212] *Ibidem.*
[213] Article 32 obliges the processor to implement appropriate security measures. See *supra* n° 27.
[214] See *infra* n° 51.
[215] Regarding the data subject's rights, see *infra* section 8.
[216] Obligations laid down in Articles 32 to 36 relate to security of personal data, including the data protection impact assessment and prior consultation. See *supra* n° 27 and n° 44.
[217] "*With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions*."
[218] Article 28.2 GDPR.
[219] *Ibidem*.

Regulation.[220] In any case, the initial processor remains fully liable to the controller for the performance of the other processor's obligations.[221]

52. **The obligation to follow the instructions** – Pursuant to the GDPR, *"[t]he processor and any other person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller; unless required to do so by Union or Member State law*."[222]

The consortium has concluded contracts with PHCT and Amazon Web Services containing all information listed above in n° 50. The consortium should document the given instructions.
As Amazon Web Services is part of the CISPE code of conduct (the code of conduct for Cloud Infrastructure Services Providers in Europe), the consortium is allowed to use these services to store data exclusively in the EU (in this case, the servers are in Germany), as it prevents the US to access these data.
PHCT and Amazon Web Services must follow the instructions from the consortium and respect their respective obligations indicated in their respective contracts.

7.5. Records of processing activities

53. **The controller's obligation to maintain a record** – The controller processing health data[223] shall maintain a record of processing activities,[224] in writing, including in electronical form.[225] This record must contain a certain number of information specified by the GDPR, namely:[226]

    (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
    (b) the purposes of the processing;
    (c) a description of the categories of data subjects and of the categories of personal data;
    (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
    (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
    (f) where possible, the envisaged time limits for erasure of the different categories of data;
    (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).[227]

54. **The processor's obligation to maintain a record** – The processor processing health data[228] shall maintain a record of all categories of processing activities carried out on behalf of the controller,[229] in writing, including in electronical form.[230] This record must contain a certain number of information specified by the GDPR, namely:[231]

[220] Article 28.4 GDPR. See *supra* n° 50.
[221] Article 28.4 GDPR.
[222] Article 29 GDPR.
[223] See Article 30.5 GDPR.
[224] Article 30.1 GDPR.
[225] Article 30.3 GDPR.
[226] Article 30.1 GDPR.
[227] See *supra* n° 27.
[228] See Article 30.5 GDPR.
[229] Article 30.2 GDPR.
[230] Article 30.3 GDPR.
[231] Article 30.2 GDPR.

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).[232]

The consortium as well as PHCT and Amazon Web Services must maintain records of processing activities containing all information listed respectively in n° 53 and n° 54, because they process health data and therefore the exception provided for organisations employing fewer than 250 persons, does not apply.

7.6. Transparency and information (obligations of the controller)

55. **A data subjects' right** – As a preliminary remark, we note that the obligations of transparency and information incumbent upon the controller are included in the GDPR chapter on the data subjects' rights.[233] We have deliberately chosen to include this right in the obligations of the controller because the information specified below[234] must be provided by the controller (or by the processor if the controller delegates this obligation) regardless of any action taken by the data subject. The transparency modalities, on their part, do not only apply to such information but also to communication with data subjects concerning the exercise of their rights[235] and in relation to data breaches.[236] Of course, the exercise of a right by the data subject also generates obligations towards the controller, but these obligations remain dependent on a request from the data subject.

56. **Transparency modalities** – The controller must take appropriate measures to provide information and communication to the data subject "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language* […]."[237] It is also specified that the information "*shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means*."[238] The controller may combine this information with "*standardised icons*" in order to give "*in an easily, intelligible and clearly legible manner a meaningful overview of the intended processing*."[239]

The GDPR obliges the controller to facilitate the exercise of the data subjects' rights.[240] In this view, information and communication must be provided free of charge, unless a request from a data

[232] See *supra* n° 27.
[233] Namely, Chapter III of the GDPR.
[234] Under Article 13 and 14 GDPR. See *infra* n° 57-58.
[235] Under Articles 15 to 22 GDPR. See *supra* section 6 and *infra* section 8.
[236] Under Article 34 GDPR. See *supra* n° 29.
[237] Article 12.1 GDPR. See Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), pp. 7-11, paras 8-16.
[238] *Ibid.*, pp. 11-13, paras 17-21.
[239] Article 12.7 GDPR. "*Where the icons are presented electronically they shall be machine-readable*."
[240] Article 12.2 GDPR.

subject is manifestly unfounded or excessive.[241] Also important to note is that the controller must verify the identity of the person making a request.[242]

Within one month upon receiving a request form the data subject, the controller must provide information on action taken on the request, or on the extension of the delay by further two months.[243] Of course, information on action taken must in the latter case be provided within the extended delay.[244] Where applicable, the controller must inform the data subject without delay and at the latest within one month upon the receipt of the request, of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and seeking judicial remedy.[245]

57. **Information to be provided where personal data are collected from the data subject** – Where personal data are collected from the data subject, the controller must provide the latter with a multiple set of information,[246] insofar the data subject has not already the information.[247] Such information must be provided at the time the personal data are obtained.[248]

In addition, the controller must communicate any subsequent substantive or material changes to this information.[249] Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected,[250] the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information listed below in points 7 to 12.[251]

While the GDPR distinguishes information that must be provided in any case[252] and other information that must only be provided where they are "*necessary to ensure fair and transparent processing*,"[253] the EDPB considers that there is no difference regarding the status of those information and that all of them must be provided to the data subject.[254] The required information are:[255]

1) the identity and the contact details of the controller and, where applicable, of the controller's representative;
2) the contact details of the data protection officer, where applicable;
3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4) where the processing is based on [legitimate interests purposes],[256] the legitimate interests pursued by the controller or by a third party;
5) the recipients or categories of recipients of the personal data, if any;

---

[241] Article 12.5 GDPR. In this case, "*the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request*."
[242] Article 12.6 GDPR.
[243] Article 12.3 GDPR.
[244] *Ibidem*.
[245] Article 12.4 GDPR.
[246] Article 13 GDPR.
[247] Article 13.4 GDPR.
[248] Article 13.1-2 GDPR.
[249] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 16, para 29.
[250] See *supra* n° 23.
[251] Article 13.3 GDPR.
[252] Article 13.1 GDPR.
[253] Article 13.2 GDPR.
[254] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 14, para 23.
[255] Article 13.1-2 GDPR (emphasis added).
[256] Under Article 6.1 (f) GDPR.

6) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available
7) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
8) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing[257] as well as the right to data portability;
9) where the processing is based on [consent],[258] the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
10) the right to lodge a complaint with a supervisory authority;
11) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
12) the existence of automated decision-making, including profiling,[259] and, at least in those cases, *meaningful information about the logic involved*, as well as the significance and the envisaged consequences of such processing for the data subject.

The latter required information is, following the provision, only required in the existence of automated decision-making based *solely* on automated processing, including profiling, that produces legal or similarly significant effects.[260] If we follow strictly this provision, the information would thus not be required in medical research and medical practice since such an automated decision-making based solely on automated processing is anyway purely prohibited.[261] However, according to the Article 29 Working Party,[262] "*[i]f the automated decision-making and profiling does not meet the Article 22(1) definition it is nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair, and meet all the other information requirements of Articles 13 and 14*." Accordingly, if the controller is making automated decisions, it must:[263]

- tell the data subject that they are engaging in this type of activity;
- provide meaningful information about the logic involved; and
- explain the significance and envisaged consequences of the processing.[264]

According to the Article 29 Working Party, "*[t]he growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works. The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm*."[265] Nevertheless, the purpose of providing information about

[257] The right to object to processing must be explicitly brought to the attention of the data subject and presented clearly and separately from any other information, pursuant to Article 21.4 GDPR.
[258] Under Article 6.1 (a) or Article 9.2 (a) GDPR.
[259] Referred to in Article 22.1 and 22.4 GDPR.
[260] Referred to in Article 22.1 and 22.4 GDPR.
[261] Article 22 GDPR. See *supra* n° 41.
[262] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (n 38), p. 25.
[263] *Ibid*., p. 25.
[264] "*In order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given*." *Ibid*., p. 26.
[265] *Ibid*., p. 25.

the logic involved is to enable the data subject to understand the processing.[266] While this would require explanations through causal relationships, machine learning systems base their results on statistical correlations.[267] It is therefore inherently impossible to provide information about the *logic* involved where machine learning techniques are used.

The Recommendation of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of profiling refers not to the 'logic involved' but to the *reasoning underlying the profiling* or the *model* used by the data controller.[268] This 'model' is defined as "*a mathematical abstraction used, for example, in automatic learning methods, which provides a simplified description of the data to solve the task to be performed*."[269] Even if providing the model used does not amount to providing the logic involved, it would enable the data subject to receive meaningful information about the processing operation. As the rationale of the GDPR provision is to ensure fair and transparent processing of personal data, it may be sufficient to provide this model where features are extracted from voice and video recording, and gait signals. However, where digital biomarkers are used for the treatment of the disease, it is crucial that the physician remains able to provide meaningful information about the logic involved in the processing operations leading to a treatment decision. Hence, understanding what the algorithm does when detecting subgroups of patients and clustering multivariate clinical and longitudinal outcome trajectories, must remain a priority for the team conducting medical research.[270]

58. **Information to be provided where personal data have been indirectly obtained** – Where personal data have not been obtained from the data subject, the controller must also provide the latter with a multiple set of information.[271] Such information must be provided at the latest within one month after obtaining the personal data,[272] or earlier, depending on the circumstance, as follows:[273]

    (a) within a reasonable period after obtaining the personal data, having regard to the specific circumstances in which the personal data are processed;
    (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
    (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

    In addition, the controller must communicate any subsequent substantive or material changes to this information.[274] Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained,[275] the controller shall provide the data

[266] The Article 29 Working Party presents this in other words: "*The information provided should, however, be sufficiently comprehensive for the data subject to understand* ***the reasons for the decision***." *Ibid*., p. 25 (emphasis added).
[267] See Y. Poullet, *Le RGPD face aux défis de l'intelligence artificielle* (n 96), p. 111, n°34.
[268] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling (n 177), point 4.1.h.
[269] *Ibid*., point 1.1.e.
[270] See *supra* n° 42.
[271] Article 14 GDPR.
[272] Article 14.3 (a) GDPR; Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), pp. 15-16, para 27.
[273] Article 14.3 GDPR.
[274] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 16, para 29.
[275] See *supra* n° 23.

subject prior to that further processing with information on that other purpose and with any relevant further information listed below in points 7 to 13.[276]

While the GDPR distinguishes information that must be provided in any case[277] and other information that must only be provided where they are "*necessary to ensure fair and transparent processing*,"[278] the EDPB considers that there is no difference between the status of those information and that all of them must be provided to the data subject.[279] The required information are:[280]

1) the identity and the contact details of the controller and, where applicable, of the controller's representative;
2) the contact details of the data protection officer, where applicable;
3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4) the categories of personal data concerned;
5) the recipients or categories of recipients of the personal data, if any;
6) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available. 2.
7) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
8) where the processing is based on point [legitimate interests purposes],[281] the legitimate interests pursued by the controller or by a third party;
9) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
10) where processing is based on [consent],[282] the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
11) the right to lodge a complaint with a supervisory authority;
12) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
13) the existence of automated decision-making, including profiling,[283] and, at least in those cases, *meaningful information about the logic involved*, as well as the significance and the envisaged consequences of such processing for the data subject.

Regarding the meaningful information to be provided about the logic involved, see our developments above.[284] Such information, like other listed information, must however not be provided insofar as:[285]

(a) the data subject already has the information;

[276] Article 14.4 GDPR.
[277] Article 14.1 GDPR.
[278] Article 14.2 GDPR.
[279] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 14, para 23.
[280] Article 14.1-2 GDPR (emphasis added).
[281] Under Article 6.1 (f) GDPR.
[282] Under Article 6.1 (a) or Article 9.2 (a) GDPR.
[283] Referred to in Article 22.1 and 22.4 GDPR.
[284] *Supra* n° 57.
[285] Article 14.5 GDPR (emphasis added).

(b) *- the provision of such information proves impossible[286] or would involve a disproportionate effort,[287] in particular for processing for archiving […] scientific […] research purposes […] or*
- in so far as the obligation [to provide information mentioned in points 1 to 6] is likely to render impossible or seriously impair the achievement of the objectives of that processing.[288]
In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

We can question why this derogation regime, which undermines the protection of personal data, is only foreseen where personal data have been indirectly obtained. Regarding the circumstances under (b), the EDPB concludes that *"[i]t therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject."*[289] Such derogations can thus not be invoked because of the difficulty to provide 'meaningful information about the logic involved' where machine learning methods are used to process personal data indirectly obtained.

The consortium must inform the data subjects regarding the processing of their personal data pursuant to the modalities detailed hereabove in n° 56-57-58.

Regarding personal data collected from PD patients by the consortium, the latter shall provide the patients concerned with the information listed above in n° 57, points 1, 2, 3, 4, 5, 7, 8, 10 and 12.
Regarding personal data that were not obtained from the PD patients by the consortium, the consortium shall provide the patients concerned with the information listed above in n° 58, points 1, 2, 3, 4, 5, 7, 8, 9, 11, 12 and 13. Providing the information is not mandatory insofar as it proves impossible; would involve a disproportionate effort; or is likely to render impossible or seriously impair the achievement of the objectives of the processing (this latter derogation only applies to points 1 to 5). The impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject. Nor does the obligation apply insofar as obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which

[286] The Article 29 Working Party noted that *"[t]he situation where it "proves impossible" under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects."* Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 29, para 59. See also p. 31, para 64.

[287] Recital 62 of the GDPR specifies in this regard that "*the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into account*." See also Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 31, para 64.

[288] The Article 29 Working Party specified that "*[t]o rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(b) presupposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis*." Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 31, para 65.

[289] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), p. 30, para 62.

provides appropriate measures to protect the data subject's legitimate interests; or where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

In order to be able to provide meaningful information about the logic involved in the decisions, understanding what the algorithm does when detecting subgroups of patients and clustering multivariate clinical and longitudinal outcome trajectories, must remain a priority in the research project. Furthermore, this is essential to enable physicians to use DMs in clinical practice while complying with their transparency obligations.

8. Rights of the data subject

59. Foreword – The patients and healthy controls (data subjects) whose health data are processed are entitled with a set of rights under the GDPR. When the data subjects exercise these rights, the controller must act accordingly. We therefore analyse hereunder these rights and to what extent the data subjects can exercise them in the context of a research project in the medical field, like the DIGIPD project (sections 8.1 to 8.6).

8.1. Right of access

60. **Right of access** – The data subject has the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed. Where that is the case, the data subject has the right to request access to the personal data and to receive a set of information.[290] This right of access can be exercised by the data subject at reasonable intervals and is foreseen to enable him or her to be aware of, and verify, the lawfulness of the processing.[291]

    It is expressly specified that the right of access "*includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided*."[292] Where the controller processes a large quantity of information concerning the data subject, "*the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates*."[293]

[290] Namely:
1) *"the purposes of the processing;*
2) *the categories of personal data concerned;*
3) *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
4) *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
5) *the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
6) *the right to lodge a complaint with a supervisory authority;*
7) *where the personal data are not collected from the data subject, any available information as to their source;*
8) *the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."* (Article 15.1 GDPR).

[291] Recital 63 GDPR.

[292] *Ibidem*.

[293] *Ibidem*.

Where the data subject exercises this right, the controller shall provide a copy of the personal data undergoing processing.[294] In accordance with the transparency modalities described above,[295] these personal data must be communicated to the data subject "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language* […]."[296]

This obligation may prove complicate as regards the features describing the characteristics of the patients which are not human-understandable[297] as well as regards the digital biomarkers. As the aim of this right of access is to enable the data subject to exercise control over the personal data relating to him or her, the researcher or physician should explain to the patient the personal data on which decisions are based, in an intelligible manner.

61. **Derogations for scientific research purposes** – However, where personal data are processed for scientific research purposes, the GDPR entitles EU and Member State law to provide for derogations from the right of access, insofar as this right is "*likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*."[298] The Belgian law provides for such a derogation regime,[299] as well as the Luxemburg law.[300]

Where requested by the data subject, the consortium shall:
- confirm as to whether personal data concerning him or her are being processed;
- provide access to the personal data;
- provide a set of information (see footnote 290);
- **provide a copy of the personal data undergoing processing.**

However, these obligations do not apply insofar as (cumulative conditions):
- they are likely to render impossible or seriously impair the achievement of the specific purposes;
- derogations are necessary for the fulfilment of those purposes;
- the applicable Member State law provides for such derogation;
- appropriate safeguards are implemented pursuant to the GDPR and the Member State law.

8.2. Right to rectification

62. **Right to rectification** – The data subject has the right to have personal data concerning him or her rectified without undue delay and, considering the purposes of the processing, to have it completed.[301]

[294] Article 15.3 GDPR.
[295] *Supra* n° 56.
[296] Article 12.1 GDPR. See Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (n 69), pp. 7-11, paras 8-16.
[297] See *supra* n° 5.
[298] Article 89.2 GDPR.
[299] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Title 4.
[300] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Articles 63 and 65.
[301] Article 16 GDPR.

63. **Notification obligation** – Consequently, the controller has the obligation to notify the rectification of personal data carried out in accordance with this right to each recipient to whom the personal data have been disclosed. This obligation does however not apply if it proves impossible or involves disproportionate effort.[302]

64. **Derogations for scientific research purposes** – However, where personal data are processed for scientific research purposes, the GDPR entitles EU and Member State law to provide for derogations from the right to rectification, insofar as this right is "*likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*."[303] The Belgian law provides for such a derogation regime,[304] as well as the Luxemburg law.[305]

Where requested by the data subject, the consortium shall:
- rectify inaccurate personal data;
- complete incomplete personal data;
- communicate the rectification of personal data to each recipient to whom the personal data have been disclosed (unless this proves impossible or involves disproportionate effort).

However, rectification is not mandatory insofar as (cumulative conditions):
- it is likely to render impossible or seriously impair the achievement of the specific purposes;
- derogations are necessary for the fulfilment of those purposes;
- the applicable Member State law provides for such derogation;
- appropriate safeguards are implemented pursuant to the GDPR and the Member State law.

8.3. Right to erasure

65. **Right to erasure** – The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where, *i.a.*:[306]
    (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;[307]
    (b) the data subject withdraws consent on which the processing is based,[308] and where there is no other legal ground for the processing; [309]

[302] Article 19 GDPR.
[303] Article 89.2 GDPR.
[304] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Title 4.
[305] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Articles 63 and 65.
[306] Article 17.1 GDPR.
[307] Article 17.1 (a) GDPR. The controller is already obliged to erase personal data that are no longer necessary in relation to the purposes for which they were collected or otherwise processed pursuant to Article 5.1 (e) GDPR. See *supra* n° 25.
[308] According to Article 6.1 (a) or Article 9.2 (a) GDPR. See *supra* n° 33-35.
[309] Article 17.1 (b) GDPR.

(c) the data subject objects to the processing[310] and there are no overriding legitimate grounds for the processing;[311]
(d) the personal data have been unlawfully processed;[312]
(e) the personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.[313]

66. **Notification obligation** – Consequently, the controller has the obligation to notify the erasure of personal data carried out in accordance with this right to each recipient to whom the personal data have been disclosed. This obligation does however not apply if it proves impossible or involves disproportionate effort.[314]

67. **Derogations for scientific research purposes** – The right to erasure is however restricted where, *i.a.*, the processing is necessary for achieving scientific research purposes insofar as it is likely to render impossible or seriously impair the achievement of the objectives of that processing.[315] In this case, further retention of the personal data is lawful.[316]

Where requested by the data subject and any of the listed grounds applies (n° 65), the consortium shall:
- erase personal data concerning him or her without undue delay;
- communicate the erasure of personal data to each recipient to whom the personal data have been disclosed (unless this proves impossible or involves disproportionate effort).

However, erasure of personal data is not mandatory insofar as:
- it is likely to render impossible or seriously impair the achievement of the specific purposes;
- appropriate safeguards are implemented pursuant to the GDPR.

8.4. Right to restriction of processing

68. **Right to restriction of processing** – The data subject has the right to obtain from the controller restriction of processing where:[317]
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;[318]
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;[319]
(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;[320]

[310] Pursuant to Article 21.1 of the GDPR. See *infra* n° 73-75.
[311] Article 17.1 (c) GDPR.
[312] Article 17.1 (d) GDPR.
[313] Article 17.1 (e) GDPR.
[314] Article 19 GDPR.
[315] Article 17.3 (d) GDPR.
[316] Recital 65 GDPR.
[317] Article 18.1 GDPR.
[318] Article 18.1 (a) GDPR.
[319] Article 18.1 (b) GDPR.
[320] Article 18.1 (c) GDPR.

(d) the data subject has objected to processing[321] pending the verification whether the legitimate grounds of the controller override those of the data subject.[322]

69. **The obligation to follow the instructions** – Pursuant to the GDPR, *"[t]he processor and any other person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller; unless required to do so by Union or Member State law*."[323]

Where processing has been restricted, the personal data concerned can only be stored and "*be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State*."[324]

70. **Notification obligation** – Consequently, the controller has the obligation to notify the restriction of processing carried out in accordance with this right to each recipient to whom the personal data have been disclosed. This obligation does however not apply if it proves impossible or involves disproportionate effort.[325] The controller must also inform the data subject before the restriction of processing is lifted.[326]

71. **Derogations for scientific research purposes** – However, where personal data are processed for scientific research purposes, the GDPR entitles EU and Member State law to provide for derogations from the right to restriction of processing, insofar as this right is "*likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*."[327] The Belgian law provides for such a derogation regime,[328] as well as the Luxemburg law.[329]

Where requested by the data subject and any of the listed grounds applies (n° 68), the consortium shall:
- stop processing the personal data concerned during the indicated period;
- communicate the restriction of processing to each recipient to whom the personal data have been disclosed (unless this proves impossible or involves disproportionate effort);
- inform the data subject before the restriction of processing is lifted.

However, restriction of processing is not mandatory insofar as (cumulative conditions):
- it is likely to render impossible or seriously impair the achievement of the specific purposes;
- derogations are necessary for the fulfilment of those purposes;
- the applicable Member State law provides for such derogation;

[321] Pursuant to Article 21.1 of the GDPR. See *infra* n° 73-75.
[322] Article 18.1 (d) GDPR.
[323] Article 29 GDPR.
[324] Article 18.2 GDPR.
[325] Article 19 GDPR.
[326] Article 18.3 GDPR.
[327] Article 89.2 GDPR.
[328] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Title 4.
[329] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Articles 63 and 65.

- appropriate safeguards are implemented pursuant to the GDPR and the Member State law.

8.5. Right to data portability

72. **A non-invokable right** – The right to portability will not be developed in this report as the data subject is only granted this right when the processing is based on consent[330] or on a contract[331].[332] As we have seen,[333] processing of health data will rather be based on the necessity of the processing for achieving scientific research purposes or purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment.

Since processing of health data by the consortium is not based on consent of the data subjects but rather on the fact that the processing is necessary to achieve scientific research purposes, the data subjects do not benefit from the right to data portability.

8.6. Right to object[334]

73. **Right to object to processing based on legitimate interests purposes** – The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on the necessity of this processing for the purposes of the legitimate interests pursued by the controller or a third party overriding the interests, rights and freedoms of the data subject[335].[336] Consequently, the controller shall demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject if it wishes to continue the processing. Otherwise, it shall no longer process the personal data, unless for the establishment, exercise, or defence of legal claims.[337]

74. **Right to object to processing carried out for scientific research purposes** – Where personal data are processed for scientific research purposes,[338] the data subject has the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her.[339]

75. **Derogations for scientific research purposes** – However, where personal data are processed for scientific research purposes, the GDPR entitles EU and Member State law to provide for derogations from the right to object, insofar as this right is "*likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the*

[330] Pursuant to Article 6.1 (a) or Article 9.2 (a) GDPR.
[331] Pursuant to Article 6.1 (b) GDPR.
[332] Article 20.1 (a) GDPR.
[333] See *supra* section 4.
[334] The data subject has also the right to object to processing of personal data concerning him or her which is based on Article 6.1 (e) and to processing of personal data for direct marketing purposes (Article 21.1-2-3). However, we only develop the rights that are applicable in the context of medical research and medical practice.
[335] Based on Article 6.1 (f) GDPR. This lawfulness basis includes the circumstances enunciated in Article 9.2 (h) and (j) and analysed *supra* n° 36-38.
[336] Article 21.1 GDPR.
[337] Article 21.1 GDPR.
[338] Pursuant to Article 89.1 GDPR.
[339] "*Unless the processing is necessary for the performance of a task carried out for reasons of public interest.*" Article 21.6 GDPR.

fulfilment of those purposes."[340] The Belgian law provides for such a derogation regime,[341] as well as the Luxemburg law.[342]

Where the data subject objects, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, the consortium shall:

- no longer process the personal data.

However, personal data can further be processed insofar as (cumulative conditions):

- the objection is likely to render impossible or seriously impair the achievement of the specific purposes;
- derogations are necessary for the fulfilment of those purposes;
- the applicable Member State law provides for such derogation;
- appropriate safeguards are implemented pursuant to the GDPR and the Member State law.

Conclusions

76. The GDPR imposes a multiple set of obligations on the controller and processor willing to process digital biomarkers for better individualised treatment of a disease. In particular, some principles and obligations may challenge the processing operations at stake, which we recall here:
    - A data protection impact assessment must be carried out, including to assess the necessity and proportionality of the processing operations in relation to the purposes (medical research or medical practice purposes). This is important to comply with the purpose limitation principle, which requires that the purposes are legitimate.
    - Accuracy of personal data must be maintained, even if features describing characteristics within an individual patient are not "human understandable". This is crucial to comply with the accuracy principle.
    - Understanding the outcomes of the processing operations is crucial as well, as digital biomarkers and the advanced analytical methods will not be usable in medical practice if a human cannot take decisions based on the outcomes. This human involvement in the treatment decisions in required because solely automated individual decision-making is prohibited.
    - This human involvement jibes with the necessity that the controller remains able to provide meaningful information about the logic involved in the processing operations leading to a decision, in order to comply with the transparency principle, and more specifically with the obligation to provide a set of information to the data subject.
    - The controller must be able to explain the personal data it processes in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is important to 'provide a copy' of the personal data where the data subject exercises the right of access.

[340] Article 89.2 GDPR.

[341] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Title 4.

[342] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, Articles 63 and 65.

Obligations of the consortium under the GDPR:

Prior to the processing operations:

- appoint a Data Protection Officer (DPO) with professional qualities and knowledge of data protection law and practice;

- draft a contract with PHCT and Amazon Web Services, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the consortium. The contracts must also indicate a series of obligations incumbent upon the processors.

Prior to the processing operations + all along the project:

- carry out a data protection impact assessment (DPIA): an assessment of the impact of the envisaged processing operations on the protection of personal data.

  The assessment must contain at least:
  - a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued by the consortium;
  - an assessment of the necessity and proportionality of the processing operations in relation to the purposes of the research project;
  - an assessment of the risks to the rights and freedoms of data subjects (PD patients);
  - the measures envisaged to:
    - address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data;
    - demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. In this line, the consortium must verify that the processors PHCT and Amazon Web Services provide sufficient guarantees to comply with the GDPR all along the project.

  In addition, the consortium shall seek the views of data subjects or their representatives on the processing → Task 5.4 DIGIPD

All along the project:

- implement appropriate technical and organisational measures to respect the data protection principles both at the time of the determination of the means for processing and at the time of the processing itself (Data protection by design and by default), namely:

- ensure transparency regarding the functions and processing of PD patients' and healthy controls' data: provide a set of information to the data subjects concerned at the time the personal data are obtained from them or within a reasonable period of maximum one month after obtaining the personal data.

  Among other information, the consortium must:
  - tell the data subject that they are engaging in this type of activity;
  - provide meaningful information about the logic involved;
    - ➔ Understanding what the algorithm does when detecting subgroups of patients and clustering multivariate clinical and longitudinal outcome trajectories, must remain a priority in the research project.
  - explain the significance and envisaged consequences of the processing.

  Information and communication must be provided to the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

  The consortium must also be able to explain the personal data it processes in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. This is important to 'provide a copy' of the personal data where the data subject exercises the right of access;

- not process personal data for purposes leading to a disproportionate interference with the rights, freedoms and interests at stake, including those of the patients and the society as a whole (→ the assessment of the proportionality is part of the data protection impact assessment). Pseudonymisation of data is a security measure that reduces these interferences.

- stop the processing of personal data that are found either inadequate, irrelevant, or unnecessary for the treatment of Parkinson's disease, and erase or anonymise these data if their further processing is not necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes;

- maintain the accuracy of all personal data that are processed, including the features that are not necessarily human understandable;

- implement high security organisational and technical measures as well as appropriate safeguards for the rights and freedoms of the patients.

  Organisational measures include limiting the number of people with access to personal data and using two-factor authentication and protecting physically the infrastructures used to process the personal data.

Technical measures include the use of a firewall and anti-virus programs, and pseudonymisation of the patients' and healthy controls' data by a trusted third party.

In case of a personal data breach likely to result in a risk to the rights and freedoms of natural persons, the consortium must notify the personal data breach to the supervisory authority and, where the risk is high, communicate the personal data breach to the data subjects.

- maintain a record of processing activities, in writing, containing:
  - the name and contact details of the consortium and the data protection officer;
  - the purposes of the processing;
  - a description of the categories of data subjects and of the categories of personal data;
  - the categories of recipients to whom the personal data have been or will be disclosed;
  - where possible, the envisaged time limits for erasure of the different categories of data;
  - where possible, a general description of the technical and organisational security measures.

- facilitate the exercise of their rights by the PD patients:
  - the right of access;
  - the right to rectification;
  - the right to erasure;
  - the right to restriction of processing;
  - the right to object.

Table of Contents