

ANNEX 1

LIST OF REQUIREMENTS UNDER THE GDPR

Introduction - General Data Protection Regulation ("GDPR")

1. The EU General Data Protection Regulation ("GDPR") will replace the current Data Protection Directive 95/46/EC and will be directly applicable from 25 May 2018 in all EU Member States.

Scope of the GDPR

2. The GDPR applies to the processing personal data and sets out the requirements on the processing of personal data. Personal data means any information relating to an identified or identifiable natural person ("data subject"); 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 identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
3. Processing means 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.
4. The GDPR applies to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. The GDPR also applies to the processing of personal data in the context of the activities of an establishment of an organisation in the European Union, regardless of whether the processing takes place in the European Union or not.
5. Genomics data are qualified as personal data within the meaning of the GDPR. The storage of genomics data (personal data) can be considered as a processing under the GDPR.

Relevant parties

6. The GDPR draws a distinction between a “data controller” and a “data processor” in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. The party which, alone or jointly with others, determines the purposes and means of the processing of personal data is called the controller, and the party which processes personal data on behalf of the controller is called the processor.
7. Below we will provide an overview of the rights and obligations of a controller under the GDPR and when relevant, additional or deviating obligations of the processor.

Data processing agreement

8. Where processing is to be carried out by a processor on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.
9. Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and sets 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. That contract or other legal act must stipulate, in particular, that the processor:
 - a. *processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country, unless required to do so by 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 technical and organisational security measures;*
 - d. *shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall 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;*
 - e. *shall impose the same data protection obligations as set out in the contract between the controller and the processor on that other sub processor;*
 - f. *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;*
 - g. *assists the controller in ensuring compliance with the obligations regarding personal data breaches taking into account the nature of processing and the information available to the processor;*

- h. *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 law requires storage of the personal data;*
- i. *makes available to the controller all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*

Requirements

10. The GDPR requires that personal data must be:¹

- a. *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
- b. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');*
- c. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
- d. *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 ('accuracy');*
- e. *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 ('storage limitation');*
- f. *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 ('integrity and confidentiality').*

11. The controller must be able to base the data processing on one of the six legal grounds provided by the GDPR:²

- a. *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
- b. *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
- c. *processing is necessary for compliance with a legal obligation to which the controller is subject;*
- d. *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
- e. *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- f. *processing is necessary for the purposes of the legitimate interests pursued by the controller*

12. Where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data. The data subject has

¹ Article 5 GDPR.

² Article 6 GDPR.

the right to withdraw his or her consent at any time. The withdrawal of consent however, does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the possibility to withdraw consent. It must be as easy to withdraw as to give consent.

Special personal data

13. The nature of some personal data entails that their processing can constitute a big intrusion of the data subject's privacy, since such data contain sensitive information about someone. The GDPR refers to such data as special personal data. The processing of special personal data is subject to a stricter regime than the processing of ordinary personal data. Special personal data are "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*"³ The principle of the GDPR is that the processing of special personal data is prohibited. The GDPR and the Implementation Act provide a number of exemptions from this prohibition, such as explicit consent of the data subject.

Exemption regarding genetic data

14. The Implementation Act contains a specific exemption to the prohibition to process genetic data. The prohibition does not apply if this processing relates to the data subject from whom the genetic data have been obtained. The processing is therefore not allowed if it relates to other data subjects in the same genetic line.
15. In other cases, the prohibition to process genetic data is not applicable, if:
 - a. a substantial public interest prevails; or
 - b. the processing is necessary for scientific research that serves a public interest or for statistical purposes, if the data subject has given explicit consent and provided that appropriate safeguards are established.

Transparency

16. A data subject whose data are processed must be able to track what happens with its data. Therefore, the GDPR contains a provision on information providing to the data subject.⁴ This provision makes a distinction in various respects between the situation in which the data is collected from the data subject himself, and the situation in the data is collected in another way.

³ Article 9 GDPR.

⁴ Article 12 GDPR.

Relevant information

17. Where personal data relating to a data subject are collected from the data subject, the controller must, at the time when personal data are obtained, provide the data subject with all of the following information:⁵
- *the identity and the contact details of the controller and, where applicable, of the controller's representative;*
 - *the contact details of the data protection officer, where applicable;*
 - *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
 - *where the processing is based on legitimate interest, the legitimate interests pursued by the controller or by a third party;*
 - *the recipients or categories of recipients of the personal data, if any;*
 - *where applicable, the fact that the controller intends to transfer personal data to a third country;*
 - *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*
 - *the existence of the right to request 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 as well as the right to data portability;*
 - *the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
 - *the right to lodge a complaint with a supervisory authority;*
 - *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;*
 - *the existence of automated decision-making, including profiling.*
18. Where personal data have not been obtained from the data subject, the controller also needs to inform the data subjects (in addition to the above) about the source from where the personal data originate, and if applicable, whether it came from publicly accessible sources.⁶ The controller must provide data subjects with this information within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed.⁷

Data subject rights

19. Data subjects have several rights that enable them to control the processing of their personal data:

⁵ Article 13 GDPR.

⁶ Article 14 GDPR.

⁷ Article 14(3)(a) GDPR.

- right of access: a data subject has the right to obtain confirmation whether its personal data are being processed; to access the data (i.e. to a copy); and to be provided with supplemental information about the processing.
 - right to rectification: data subjects can require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, a data subject can require the controller to complete the data, or to record a supplementary statement.
 - right to erasure (right to be forgotten): data subjects have the right to have their data “erased” in certain specified situations - in essence where the processing fails to satisfy the requirements of the GDPR.
 - right to restriction of processing: a data subject can require the controller to “restrict” processing of the personal data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the data subject objects to erasure.
 - right to data portability: data portability requires the controller to provide information in a structured, commonly used and machine readable form. Further, the controller can be required to transmit the data directly to another controller
 - right to object: the data subject may object to specific types of processing, such as direct marketing, processing based on legitimate interests, and processing for research or statistical purposes.
 - right to withdraw consent: the data subject must have the right to withdraw consent at any time.
 - right not to be subject to a decision based solely on automated processing, including profiling.
20. In the event data made public by a controller is thereafter subject to a right to rectification, erasure or restriction request, the controller is required to notify each recipient of the disclosed personal data. The controller must furthermore inform the data subject about those recipients in the event this is requested by the data subject.

Records of processing activities

21. In order to demonstrate compliance with the GDPR, a controller must maintain records of processing activities under its responsibility. That record must contain all of the following information:
- a. the name and contact details of the controller and, where applicable, 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;
 - 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.
22. When performing processing activities (also) in a role as processor, the processor has to keep separate records of those processing activities. That record must contain the following information:
- a. the name and contact details of the processor
 - b. the name and contact details of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's data protection officer;
 - c. the categories of processing carried out on behalf of each controller;
 - d. where applicable, transfers of personal data to a third country, including the identification of that third country and the documentation of suitable safeguards;
 - e. where possible, a general description of the technical and organisational security measures.

Data Protection Officer

23. The controller and the processor must designate a data protection officer in any case where (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data.

Scientific research

24. The GDPR also applies to the processing of personal data for scientific research purposes. According to the GDPR, the processing of personal data for scientific research purposes may be interpreted in a broad manner. Scientific research purposes also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in

particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes.⁸

25. The processing of personal data for scientific research purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to the GDPR. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. Those measures may include pseudonimisation, if possible. 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.⁹
26. Where personal data are processed by institutions or services for scientific purposes in the public interest, and the necessary arrangements have been made to ensure that the personal data can only be used for scientific purposes, the right of access by the data subject (article 15), the right to rectification (article 16), and the right to restriction of processing (article 18) do not apply.¹⁰

⁸ Consideration 159, GDPR.

⁹ Article 89(1) GDPR.

¹⁰ Article 44, GDPR Implementation Act.