GDPR – FACTSHEET

GDPR stands for General Data Protection Regulation

GDPR is about on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

GDPR strengthens and harmonises the rules for protecting individuals' privacy rights and freedoms within and, under certain conditions, outside the EU territory.

GDPR is expected to reduce todays (Data Protection Directive) legal fragmentation, complexities and uncertainties and yet, the main principles remain the same as under the previous Directive.

What is new? Many questions and few answers at the moment
Data Subjects Rights
Breach notification
Right to access
Right to be forgotten
Data Portability

What is personal data? Definitions of personal data
Genetic data is defined in Art 34:
Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

Health data is defined in Art 35:
Personal data concerning health 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. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Art 33: It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the

opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Art 38: Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

Security of personal data

Art 39: Any processing of personal data should be lawful and fair. It 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. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. **The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.** This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. 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. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept 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. The result of pseudonymisation is pseudonymised data which remain personal data but being protected through coding or encryption.

Pseudonymisation is promoted and shall be implemented, as far and as soon as possible, in personal data processing for scientific research purposes, as a standard data protection practice.

Anonymous data are defined in GDPR as information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that

the data subject is not or no longer identifiable. Handling of anonymous data are outside the remit of GDPR. The process of “making” anonymous data are regulated by GDPR.

Privacy by Design
It will be mandatory to have the best privacy settings in all systems.

What is old?
Informed Consent from subjects/informants/patients
Controller:
The organization or person who determines the purpose for which the personal data are to be processed, and the manner in which this is to be done. The data controller is responsible for ensuring that the data are processed in accordance with the provisions of the Personal Data Act.

Data processor:
The organization or person who processes personal data on behalf of the data controller. The data processor must process the personal data only as specifically agreed with the data controller.

Data Protection Officers:

Overview of projects:

What else?
Changes to other regulations will come as a consequence of GDPR