The European Union General Data Protection Regulations (GDPR)

Michel ARNOULT

2017/july

Kayentis
Dedicated to eCOA & Patient Engagement

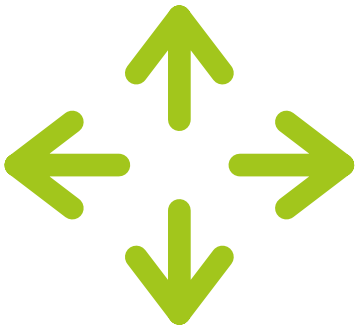
Michel ARNOULT, Consultant in Data Collection
and Data Management in Clinical Research

Contents

Introduction

The European Union (EU) Data Protection Regulations (GPDR), effective from 27 April 2016, will apply to all organisations responsible for data processing, and any sub-contractors, from 25 May 2018. These regulations replace the Data Protection Directive (Directive 95/46/EC). These regulations will apply to all EU states, which will also be able to comply with local regulations.

The EU GDPR will significantly change the management and storage of personal data by imposing new obligations and better practices on applicable organisations.



1 The fundamental changes of the EU GDPR

Privacy by design and Privacy by default

- The management of all personal data will have to be designed in line with the requirements of data protection ('Privacy by Design').
- Data collection will have to be restricted to data that are absolutely necessary for the objectives of the processing ('Privacy by Default').

Explicit consent, right of access, and the 'right to be forgotten' (data erasure)

- The arrangements should allow any affected individual to remove his/her consent and to exercise his/her 'right to be forgotten' by asking for his/her data to be erased.

Data portability

- The owner of the 'Subject data' will be able to ask the organisation responsible for the processing to transfer all data to a third party (e.g. in the event of a change in the email provider).
- The organisation responsible for the processing is advised to request proof of identity from the individual requesting the data in order to avoid fraud. This could be important in the event of the transmission of data to an unauthorised third party.

Any 'data breach' (e.g. due to flood or unauthorised access) will have to be reported to the Data Protection Authority (in France this is the CNIL) within 72 hours.

- There will be the possibility of fines of up to 4% of the turnover.

Geographical zones are extended beyond the EU.

- e.g. a US company collecting data from EU citizens and managing these data in Asia.

The nomination of an 'independent' Data Protection Officer (either internal or a third-party).

- This is an evolution of the role fulfilled in France by the Correspondant Informatique et Libertés (CIL).

The idea of joint responsability between the 'Data Controller' (responsible for the processing itself, e.g. the Sponsor) and the 'Data Processor' (e.g. a Contract Research Organisation [CRO]).

- Any organisation could fulfil both roles in parallel.
- In the event of a fine, the sanctioned organisation could refer to its work order or a sub-contractor.

The idea of 'pseudonymisation' (in addition to anonymisation and encryption), particularly in the case of sensitive data (e.g. health data, pharmacovigilance data, clinical trials data).

Impact and risk analysis (Data Protection Impact Assessment) and large scale 'inventory' of all applications concerned by personal data.

- Applications, volume.
- Duration of processing and storage.
- Geographical zone.
- Sub-contractors.
- Contracts.

Regular review and supervision of data (e.g. processing, conformity, data flow, management of access, sub-contractors, contacts) and dialogue between the Data Protection Officer and the authorities in charge of the protection of personal data (Data Protection Authority).

Adaptation of processes (and of roles and responsibilities) and of applications if necessary in order to demonstrate conformity (e.g. contracts, documentation, pre-defined list of measures).

Implementation of a process (procedure, responsible person) in the event of an incident ('Data Breach').

- Notification of the authorities within 72 hours after the incident.
- Inform any 'Data Subjects' who are victims of the 'Data Breach'.

2. New obligations for sub-contractors (e.g. data hosting, Data Processor)

The data hosting service (Data Processor) will be subject to the following obligations:

- The use of further sub-contracting by a sub-contractor is subject to prior specific written authorisation from the organisation responsible for the processing (art. 28).
- The maintenance of a register of all processing activity categories used for the responsible organisation (Data Controller) (art. 30).
- Cooperation with the Control Authority (art. 31).
- The implementation of appropriate technical and organisational measures in order to guarantee a level of security that corresponds to the risk (art. 32).
- The notification of the organisation responsible for the processing of any personal data breach as soon as possible after having become aware of the breach (art. 33).
- The designation of a delegate to the protection of individuals under certain conditions (art. 37) (4).
- Conformity to the rules governing the transfer of data outside the EU (art. 44).

The data hosting contact will have to anticipate the following roles of the sub-contractor (art. 28):

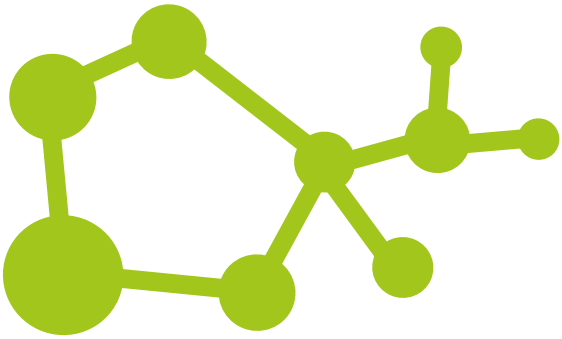
- The development of unique processing dependent on the instruction of the organisation responsible for the processing.
- The employment of individuals who are accountable, either by convention or by legal obligation, to confidentiality.

- The development of the necessary security measures.
- Request for prior authorisation of the organisation responsible for all sub-contracting.
- The creation of the technical and organisational conditions that are necessary to allow the responsible organisation to pass on its responsibility to the individuals concerned and to ensure a robust handover.
- To guarantee the obligations included in articles 32 to 36 (data security, notifications of any violation of personal data, impact analysis, prior consultation).
- Deletion or return of data at the end of the contract.
- Make available all necessary information to the responsible organisation and the Control Authority.

The data hosting service will be directly responsible, and accountable to the Control Authority, in addition to their possible civil and legal responsibility that could result from deviations from their agreement.

In practical terms, the maintenance of a registry, the notification of any personal data violations, and the designation of a delegate for data protection are the minimum measures that should be put in place by the data hosting service.

During the production of data hosting contracts it would also be useful to define in advance any further assistance that may be provided by the data hosting service to its client (the responsible organisation) regarding the rights of the individuals and regarding its obligations related to data security, the notification of personal data violations, and impact analysis.



3. The GDPR and its regulatory specificities for the Life Sciences

The GDPR considers all health data ('Data Concerning Health') as sensitive data ('Sensitive Personal Data'). These sensitive data, which can include genetic, biometric, and other health data, can be subject to specific uses by EU member states regarding their processing.

The GDPR stipulates that the use of these data in the context of scientific research is possible as long as consent is obtained and/or specific measures such as pseudonymisation are in place.

The specific needs of scientific research and public health can reduce the scope of the GDPR in terms of the 'right to be forgotten' and the erasure of data. They can also affect the areas of consent (e.g. secondary processing of data that was not planned at the time of the original consent).

In France, good practice (or codes of conduct) published by the authority in charge of the protection of personal data (CNIL MR001 & MR003) simplify the implementation of clinical trials and observational studies.

Recommendations

The organisation's team in charge of the GDPR programme should include several areas of expertise (e.g. IT, data management, regulatory, legal, quality assurance, Data privacy manager or Data Privacy Officer [if this role exists]) with the support of the General Management in order that the following steps are followed:

Implement a programme and put a team together.

- Identify the different roles that are involved in the company (e.g. General Management, Human Resources, quality, legal, IT) and in partner companies (e.g. accounts, sub-contractors).
- Allocate budget and resource (based on the implementation date of 25 May 2018).
- Appoint a Data Protection Officer (either internal or a contractor).
- Define the aims and objectives of the programme.

Evaluate the risks and train the team members and other stakeholders on the regulations and what is involved.

- Prepare the inventory and describe the process for the collection and processing of personal data.

  - e.g. identify sub-contractors.
- Estimate the risks and identify any tools that are missing for data management.
- Complete or write the procedures, document the processes.

- Explain to and train all stakeholders (and any partners, as necessary).

Create and implement the modified measures.

- Collect and manage consents.
- Manage data transfer and the relations with third parties.

  - Update contracts.
- Define the protection of individuals' rights.
- Implement (or complete) measures for data protection (e.g. physical access to data, technical aspects [e.g. anonymisation, encryption]), contacts, plans, standard operating procedures (SOPs).

Manage and improve the measures.

- Analyse the management of sensitive data, implement a regular review.
- Manage data archiving, data retention and erasing.
- Ensure data integrity and quality.
- Prepare an remediation plan in case of an incident (Data Breach).

Continuously demonstrate conformity.

- Evaluate and audit the effectiveness of the measures.
- Check the internal and external reporting periodically.
- Improve the information text and check mechanisms to resolve disputes/lawsuits.
- Prepare for any certification that may be necessary.

By the time of the implementation of the GPDR, therefore, companies involved in the life sciences must produce an inventory of their practices and review any contractual agreements with their partners (e.g. CROs, service and/or data collection solution providers, data hosting services) in order to check their conformity with GPDR and with the good practices promoted by the personal data protection authorities.

Glossary

Binding Corporate Rules (BCRs) - a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation)

Biometric Data - any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification

Consent - freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Concerning Health - any personal data related to the physical or mental health of an individual or the provision of health services to them

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject - a natural person whose personal data is processed by a controller or processor

Delegated Acts - non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity

Derogation - an exemption from a law

Directive - a legislative act that sets out a goal that all EU countries must achieve through their own national laws

Encrypted Data - personal data that are protected through technological measures to ensure that the data is only accessible/ readable by those with specified access

Enterprise - any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

Filing System - any specific set of personal data that is accessible according to specific criteria, or able to be queried

Genetic Data - data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual

Group of Undertakings - a controlling undertaking and its controlled undertakings

Joint Controllers - Article 26 of the GDPR sets out the responsibilities and liabilities of parties as "joint controllers" e.g. *the line between a sponsor's responsibilities and those of the CRO can often be blurred.*

Main Establishment - the place within the Union where the main decisions surrounding data processing are made; with regard to the processor.

Personal Data - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person (⇔ Personally Identifiable Information (PII) in the US) e.g. *names, addresses, phone numbers, account numbers, email addresses, IP addresses*).

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stay separate to ensure non-attribution

Recipient - entity to which the personal data are disclosed

Regulation - a binding legislative act that must be applied in its entirety across the Union

Representative - any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities

Right to be Forgotten - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Sensitive Personal Data - personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Supervisory Authority - a public authority which is established by a member state in accordance with article 46

References

[1] Directive 95/46/EC, 24 October 1995:
- o http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046

[2] EU Model Contracts for the transfer of personal data to third countries:
- o http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

[3] Privacy shield overview: Pharmaceutical and Medicinal Products:
- o https://www.privacyshield.gov/article?id=14-Pharmaceutical-and-Medical-Products

[4] Official Journal of the European Union L119 Volume 59, 4 May 2016:
- o http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[5] Article 29 Working Party (Guidelines):
- o http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- o http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
- o http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf

[6] European Patients Forum position on Data Protection
- o http://www.eu-patient.eu/whatwedo/Policy/Data-Protection/
- o http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf

Panacee - July 2017

Kayentis

Dedicated to eCOA & Patient Engagement