ONTIER

21th February 2017
#7

Index

DATA PROTECTION BY DESIGN AND BY DEFAULT

The General Data Protection Regulation formally introduces the concepts of privacy by design and privacy by default. In summary, **privacy by design** means that data protection should be considered prior to the development of a new product or service that requires the processing of personal data.
On the other hand, **privacy by default** implies that the tougher privacy settings are implemented once a new product or service (which involves processing data) is made available to a data subject. Only the minimum and necessary personal data for each specific purpose is processed and it is not disclosed more widely than necessary.

Current situation

Although the idea of privacy by design and privacy by default seems an innovation, it is not completely new. Directive 95/46/EC already contained provisions towards the promotion of privacy by design and by default, stating, for instance that *(…) the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures must be taken, both at the time of the design of the processing system and at the time of the processing itself, (…) whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected (…)".*

Furthermore, the Directive already establishes general principles concerning data quality and the confidentiality of the processing, in particular, the principle of good faith, lawfulness, purpose limitation, relevance, accuracy, limit of storage, among others. These principles are inherent and form the base of the new concepts.

What's new?

The GDPR formally introduces the concepts of privacy by design and privacy by default given the fact that the Directive has not been sufficient in ensuring the application of these concepts and consequently, protecting the rights of data subjects.

Under the GDPR, in particular Article 25,the Data Controller, at the time of determining the means for processing and at the time of the processing itself, **by design**, has to implement appropriate technical and security measures in order to meet the requirements of the GDPR and protect the rights of data subjects, bearing in mind:

(i) the state of the art/availability of the technology;

(ii) the cost of the implementation of the measures;

(iii) the nature, scope, context and purposes of the data processing; and

(iv) the risks of varying, likelihood and severity for the rights and freedoms of the data subject.

The GDPR expressly suggests pseudonymisation (the technique of processing data so that it can no longer be attributed to a specific person) as an effective technical and security measure to ensure appropriate safeguards are implemented in the processing of data and protecting the rights of data subjects.

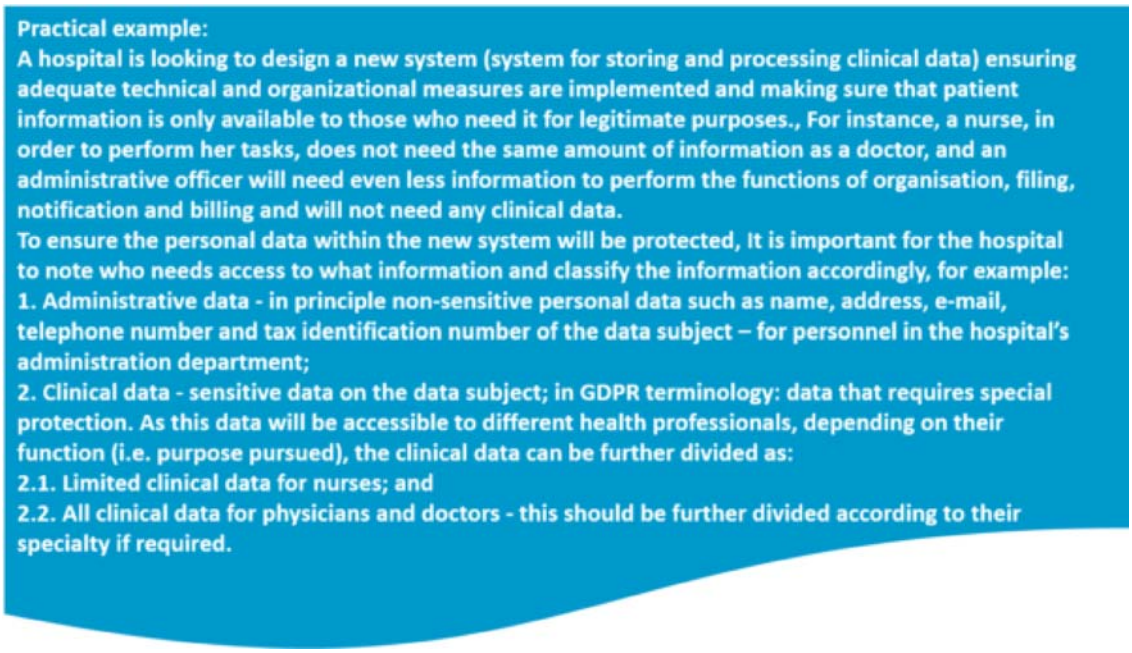
By default, the controller must implement appropriate technical and organisational measures for ensuring that only personal data that are necessary for each specific purpose of the processing are processed. This involves analysing the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Furthermore, the Data Controller must ensure that, by default, personal data is not accessible to an indefinite number of natural persons without the data subject's intervention. Under this concept, the data subject is protected by the toughest privacy settings.

These concepts are consistent with the principles relating to the processing of personal data established in the GDPR, such as data minimisation, purpose limitation, among others.

The Data Controller is also required to demonstrate compliance with these concepts and consequently, the GDPR provides for a voluntary certification that may be used to demonstrate compliance with privacy by design and by default and that will be subject to specific analysis in another chapter of this Guide. For that reason, this Chapter will not be discussing the certification process in detail.

What to do to adapt?

Data Controllers must comply with all the requirements mentioned in this Chapter. From scratch, the means for processing as well as the purposes of the processing of personal data have to be considered carefully with data protection in mind and the strictest privacy settings have to be implemented once a new product or service (which involves data processing) is made available to a data subject.



Practical example:
A hospital is looking to design a new system (system for storing and processing clinical data) ensuring adequate technical and organizational measures are implemented and making sure that patient information is only available to those who need it for legitimate purposes., For instance, a nurse, in order to perform her tasks, does not need the same amount of information as a doctor, and an administrative officer will need even less information to perform the functions of organisation, filing, notification and billing and will not need any clinical data.
To ensure the personal data within the new system will be protected, It is important for the hospital to note who needs access to what information and classify the information accordingly, for example:
1. Administrative data - in principle non-sensitive personal data such as name, address, e-mail, telephone number and tax identification number of the data subject – for personnel in the hospital's administration department;

2. Clinical data - sensitive data on the data subject; in GDPR terminology: data that requires special protection. As this data will be accessible to different health professionals, depending on their function (i.e. purpose pursued), the clinical data can be further divided as:

2.1. Limited clinical data for nurses; and

2.2. All clinical data for physicians and doctors - this should be further divided according to their specialty if required.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Ana Rocha (Portugal)
Ana Festas Henriques (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

Read more:

about us

Share on:

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A, 4º piso - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / ITALY / MEXICO / PERU / VENEZUELA
