Data Protection

Informative Text for National Contact Points in Cross-border Healthcare

Funded by the Health Programme
Of the European Union

General Data Protection Regulation

As from 25 May 2018, the new **General Data Protection Regulation** (GDPR) entered into force.
The Regulation will be directly applicable in all EU Member States.
The GDPR applies to every company or organisation that maintains or processes personal data (of clients, patients, own staff,...).
Non-compliance with the new legal framework for data protection, will have severe consequences.

- **General Data Protection Regulation (EU) 2016/679 (GDPR)**
- **25 May 2018**
- **Personal data maintenance and processing**
- **All organisations within the EU**
- **Regardless of the place of processing !**
- **Severe fines for infringements**

This brochure is intended for *National Contact Points in Cross-border Healthcare* (NCPs).

The regulation of data protection is complex and asks for special attention and resources within every organisation in the EU. This brochure is intended as a guide for NCPs, to set out the general framework of the GDPR and to emphasize the preliminary necessary measures to be taken.

Underlying document should by no means be considered as a an exhaustive list of regulatory changes and legal requirements under the GDPR. A selective overview of key areas that should be taken into consideration by all NCPs is provided. It is within the duty of NCPs to make sure they are in line with the requirements under the GDPR as from 25 May 2018.

ECORYS KU LEUVEN GfK

I. Scope of application

"The Processing of Personal Data"

- ✓ ***Processing*** = collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, ...

- ✓ ***Personal data*** = any information relating to an identified or identifiable natural person ("**data subject**"), such as a name, identification number, location data, online identifier,.... and health data.

Health data

= sensitive personal data, asking for extra protection

= processing of health data is prohibited, unless under specific circumstances, such as explicit consent of the data subject

I. Scope of application

→ **Processing + personal data = application of the GDPR**

The NCP is….. *and/or…….*

- "**Controller**": the NCP determines the purposes and means of the processing of personal data

- "**Processor**": the NCP processes personal data on behalf of the controller

II. Requirements

To be GDPR compliant, personal data should be ….

- ✓ Processed **lawfully**, **fairly** and in a **transparent manner** in relation to the data subject
- ✓ Collected for **specified, explicit and legitimate purposes**
- ✓ **Adequate, relevant** and **limited** to what is necessary in relation to the purposes
- ✓ **Accurate** and, where necessary, **kept up to date**
- ✓ **Kept for no longer than is necessary** in relation to the purposes
- ✓ Processed in a manner that ensures **appropriate security** of the personal

II. Requirements

To be GDPR compliant, the controller is accountable for …

- ✓ Ensuring **security by design and by default**
- ✓ **Minimising data** processing, in relation to the purposes
- ✓ **Keeping records** (written or electronic) of the personal data processing activities
  - Not obliged for an organisation employing fewer than 250 persons, UNLESS the processing:
    - is likely to result in a risk to the rights and freedoms of data subjects
    - is not occasional
    - includes special categories of data, such as **health data**
- ✓ Data protection **impact assessment**, whenever a type of processing, in particular using new technologies, is likely to result in a **high risk**
  - Required, amongst others, when processing on a large scale of sensitive data, such as **health data**

II. Requirements

To be GDPR compliant, the controller is accountable for …

- ✓ Drafting **privacy notices**
- ✓ **Awareness-raising and training of staff** involved in processing operations
- ✓ Providing **a system that secures personal data** in a manner that takes account of the potential risks involved for the interests and rights of the data subject
- ✓ **Mandatory data breach notifications** to the supervisory authority
- ✓ Compliance with the **communication requirements** towards data subjects regarding the processing of personal data (such as clear and plain language, transparency, easy access,…)
- ✓ Protect **data subject rights**
- ✓ ….

Requires the comprehensive review of application forms, feedback and complaints procedures, website terms and conditions, cookies policy,… !

II. Requirements

The processor is responsible for…

- ✓ Providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing is in compliance with the GDPR
- ✓ Ensuring the protection of the data subject's rights
- ✓ Processing the personal data only on documented instructions from the controller
- ✓ Not engaging a sub-processor, unless authorisation of the controller
- ✓ Making sure that at the choice of the controller, all personal data are deleted or returned to the controller after the end of the provision of services
- ✓ Providing a secure system and having a clear policy on notification in case of personal data breach
- ✓ .....

The processor ensures a secure system and policy for the detection of **data breach**. In case of high risks following from data breach, the supervising authority is notified without undue delay and at any within 72hours after detection.

II. Requirements

NCPs are obliged to designate a Data Protection Officer (DPO)

A **DPO** must be designated in any case where....

- the processing is carried out by a **public authority or body**
- the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data, such as **data concerning health**

Tasks of the **DPO**:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR
- monitor compliance with the data protection regulation
- provide advice on the data protection impact assessment and monitor its performance
- cooperate with the supervising authority
- act as contact point

*The task of DPO can be designated **internally, to an employee** (as long as there are no conflicts of interest) or **externally, to a third party**. A **single DPO** can work for multiple related institutions or departments within an organisation.*

III. Lawfulness of processing

Legal grounds for the lawful processing of personal data (patients, NCP staff, other stakeholders,…):

1. **Consent of the data subject**

Each consent should be given by a clear affirmative act (= active) establishing a consent that is free, informed, specific and revocable at any moment

Stricter requirements for protection of personal data of children

NCP website:

- Cookies consent banner
- **Prohibition of pre-ticked opt-in checkboxes**
- Clear references to terms and conditions
- ….

2. The processing is **necessary**

- for the performance of a **contract** to which the data subject is party
- for compliance with a **legal obligation** to which the controller is subject
- in order to protect the **vital interests of the data subject**
- for the performance of a task carried out in in the **public interest** or in the exercise of **official authority** vested in the controller
- for the purposes of the **legitimate interests** pursued

IV. Rights of data subjects

Right to be informed

NCPs will have to provide transparent information to the data subject on the identity of the controller, on which data will be processed, as well as on the purposes of the processing, the period of storage, the data subject's rights,... This information must be provided in easily accessible and easy to understand manner, using clear and plain language.

Right of access

The data subject has the right to obtain from the controller confirmation as to whether or not personal data are being processed.
The controller must provide a copy of the personal data undergoing processing, free of charge and within a month after request (two months extendable).

Data subject

Right to rectification and erasure

The data subject has the right to obtain rectification of inaccurate personal data concerning him or her. Besides, the data subject can request for erasure of personal data ("right to be forgotten"). The GDPR stipulates the circumstances under which a request to erasure can't be refused, except for in certain cases. Each request to rectification or erasure needs to be answered without undue delay and in any event within one month (two months extendable).

Right to portability

The data subject has the right to ask for his or her personal data in order to transmit those data to another controller. The first controller only has to provide personal data provided by the data subject him or herself. The data should be provided in a structured, commonly used and machine-readable format.

IV. Rights of data subjects

Right to object

The data subject has the right to object at any time to processing of personal data concerning him or her. More specifically, the data subject can object against data processing in certain cases, amongst which in case of direct marketing.
The data subject has to be informed on his or her right to object. This information is presented clearly and separately from any other information

Data subject

Automated individual decision making

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling. The GDPR stipulates the rights of data subjects in case of automated processing, namely the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
This right does not apply when the decision is 1° necessary for the performance of a contract, 2° is authorised or 3° is based on the explicit consent of the data subject.

V. To Do

Non-GDPR compliance can lead to administrative fines of up to 20,000,000 EUR or, in case of an undertaking, up to 4 % of the total worldwide annual turnover (the highest of both will apply).

NCPS shall make sure that…

- ✓ they are GDPR compliance
- ✓ a clear internal policy on data protection is established
- ✓ a data protection officer is designated
- ✓ any personal data are processed in a lawful and transparent manner, and only processed within the limits of the processing purposes
- ✓ processed data are carefully registered
- ✓ consent of data subjects is obtained in line with the requirements under the GDPR
- ✓ application forms, feedback and complaints procedures, website terms and conditions, cookies policy,… are comprehensively reviewed to ensure GDPR compliance
- ✓ …..