General Data Protection Regulation (GDPR)

12 Common Questions

Frontline
IT Consultancy

Frontline
IT Consultancy

GDPR

General Data Protection Regulation (GDPR) - An Overview

Frontline has been a hosting provider for many years and over recent years has become ISO 27001 accredited to ensure that our Information Security policies and procedures adhere and align to the Data Protection Act 1998.

Since the start of 2017, Frontline has been focussed on preparation for GDPR which comes into full effect on May 25th 2018. Following regular engagement with our customers, here are the 12 most commonly discussed points around GDPR, with the summarised responses or actual extracts from the regulation itself:

1. What is it:

a. A regulation designed to protect 'personal data', which is any personally identifiable information (PII) held or stored on individuals within the EU.

2. GDPR scope and definition of personal data:

a. This regulation applies to all companies, businesses or organisations worldwide that process personal data of citizens within the EU, in this regard, it is the first global data protection law.

i. Article 2 of GDPR now stipulates the scope as:

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

ii. Article 4 includes the following definition:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an
2. identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an
3. identifier such as a name, an identification number, location data, an online identifier or to one or more factors
4. specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Frontline
IT Consultancy

GDPR

3. Obtaining consent to use personal data / PII:

a. Consent must be given to use personal data and the data controller / data processor must be able to provide evidence that consent has been given

b. Simple language must be used when asking for consent

c. Clarity needs to be provided on how the information will be used

d. Silence or inactivity can no longer be assumed as consent

e. Data controller / processor MUST be able to prove clear and affirmative consent to process that data (Art 4, ref 11)

4. Data Protection Officer:

a. Is required as defined in section 4, Article 37 and will be responsible when processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating.

b. Any company who depends on processing of personal information will have to appoint a DPO (it is estimated that almost 30,000 new roles will become available for this one reason only).

c. The position of the DPO is outlined in Article 38, this includes:

   i. Involvement in a timely manner for all issues relating to the protection of personal data

   ii. Having resource provided to carry out tasks as well as having access to personal data processing operations

   iii. Not being penalised for performing duties as defined and as such will not report to the controller or processor

   iv. Receive communication from data subjects

   v. Being bound by secrecy / confidentiality concerning the performance of his or her duties

   vi. Performing other duties that do not result in a conflict of interest

d. DPO's tasks includes the following (as per Article 39):

   i. To inform and advise

   ii. To monitor compliance

   iii. To provide advice

   iv. To cooperate

   v. To act as the contact point

Frontline
IT Consultancy

GDPR

5. Data Protection Impact Assessment (or privacy impact assessment):

a. As per reference 91, a mandatory DPIA / PIA must be performed when:

i. monitoring publicly accessible areas on a large scale

ii. competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects

b. It is mandatory to conduct a DPIA before any project or piece of work that pertains to personal data as per Article 35

6. Personal data breach notification:

a. As per reference 85 and Article 33, the data controller has 72 hours to notify the supervisory authority

b. As per reference 87, technological protection and organisational measures should be in place and evidenced (this may help reduce potential fines if the notification timeframe is not met), this is further outlined in Article 32

c. As per reference 88, a defined procedure / approach / response enables full identification of who must be informed (i.e. law enforcement)

d. Article 33 defines all requirements for notifying a personal data breach to the supervisory authority

e. Article 34 further defines activities and responsibilities for communication of a personal data breach to the data subject

7. Rights of access by the data subject:

a. As per Article 15, the data subject has the right to request from the controller whether personal data pertaining to him or her is being processed, access to the personal data as well as:

i. Purpose of processing

ii. Categories of personal data concerned

iii. Recipients or categories of recipients the personal data has or will be disclosed to (in particular the countries / organisations)

iv. Period the data will be stored

v. Existence of the right to request rectification or erasure of personal data or restriction of processing (concerning the data subject) by the controller

vi. The right to lodge a complaint with the supervisory authority

vii. What source the information was collected from (if not the data subject)

viii. Any automated decision making or profiling processes employed

ix. Informed of appropriate measures taken during data transfer

Frontline
IT Consultancy

GDPR

8. Right to erasure (the right to be forgotten)

a. As per article 17, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

   i. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   ii. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

   iii. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

   iv. the personal data have been unlawfully processed

   v. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

   vi. the personal data have been collected in relation to the offer of information society services referred to in Article 8 (1).

b. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

c. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

   i. for exercising the right of freedom of expression and information;

   ii. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

   iii. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

   iv. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

   v. for the establishment, exercise or defence of legal claims.

d. As per article 19, the controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Frontline
IT Consultancy

GDPR

9. Right to rectification:

a. As defined in Article 16, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

10. Expanded liability:

a. The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

11. Data protection by design and by default (also known as Privacy by Design):

a. As described in Article 25, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

b. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

12. General conditions for imposing administrative fines:

a. Article 83 clearly outlines the financial implication for regulation infringement, specifically of interest are:

i. Reference 4, up to €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher)

1. Enforced if the obligations of the controller, processor, certification body or monitoring body are not satisfied

ii. Reference 5, up to €20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher)

1. Enforced if basic principles for processing (including consent), subjects' rights, inappropriate transfer of personal data or legal obligations for processing non-compliance are violated

Head Office

Frontline House,
Epsom Avenue,
Brooke Park Estate,
Wilmslow,
Cheshire, SK9 3PW

Frontline
IT Consultancy

Southern Office

Frontline Consultancy,
Gravel Hill Road,
Farnham, GU10 4LG

0333 323 2141

info@frontline-consultancy.co.uk
frontline-consultancy.com