GDPR 2016/679

The General Data Protection Regulation (GDPR), entered into force in April 2016 following its publication in the Official Journal of the European Union, is applicable from May 2018 and is mandatory in all its elements and directly applicable in each of the Member States. The regulation establishes rules concerning the protection of natural people with regard to the processing of personal data as well as rules concerning the free movement of such data.

GENERAL DATA PROTECTION REGULATION 2016/679

The II GDPR 2016/679 protects the rights and the fundamental freedoms of the natural people, in particular the right to the protection of personal data.

What are personal data? The **personal data is any information regarding a physical person, identified or identifiable through information** such as the name, an identification number, location data, an online identifier or one or more characteristic elements of its physical identity, physiological, genetic, psychic, economic, cultural or social.

The rule applies independently if the process is carried out on EU territory: this means which it also concerns to the data controller not established in the EU but in a place subject to the law of a Member State under international public law.

Involved subjects:

- **natural person or data owner**
- **processor**
- **controller**
- **responsible for data protection**
- **Data Protection Guarantee**
- **European Data Protection Commission.**

The natural person becomes the interested subject, which with the Regulation obtains a series of rights, such as:

- **data breach:** the Notify to the supervisory authority and to the data subject the personal data breach, without undue delay
- **right to be forgotten:** the right of the data subject to obtain the erasure of personal data
- **right to data portability:** the right of data subject to personal data transfer
- **right to access to personal data:** the right of data subject to request and obtain their personal data and information on the processing
- **right to object:** the right of data subject to request the time limit withdrawal of the processing
- **right of processing restriction:** the right of data subject to request the restriction of the processing
- **right of rectification:** the right of data subject to modify their personal data.

The important point of GDPR are:

- personal data
- data transfer to the foreign countries
- data portability
- consent
- privacy impact assessment (PIA)
- privacy by default and privacy by design
- data protection officer
- data breach notification
- right to the erasure of data "right to be forgotten"
- security of personal data.

The **main steps** that companies must take to be compliance with the provisions of the GDPR can be summarized as follows:

1. **check what you do** and what you are doing (assessment with "As is" analysis)
2. **risk assessment and PIA** (evaluation of the impact on privacy, risk analysis, classification of data etc)
3. **gap analysis**
4. **remediation plan**
5. **designations** and roles of the involved subjects (ex. Controller, Processor, Authorized subjects, Responsible of the data protection/DPO if anticipated etc.)
6. information/**training** of the personnel involved
7. **periodic update** of the system.

The controller who does not comply with the provisions of the GDPR may incur administrative sanctions (up to € 20,000,000 for companies, up to 4% of the total annual worldwide turnover, if higher), civil and/or criminal.

RINA, offers to the organizations different services, in relation to the company context and the sector it belongs to:

- **gap analysis on the GDPR**
- **personnel certification according to UNI 11697 standard**
- **training**
- **certifications in the IT sector according to ISO 27001, ISO 20000 and ISO 22301 standards etc** (as tools to support information security and data protection).

RINA Services
Via Corsica, 12
16128 Genova - Italy

T. +39 010 53851
info@rina.org

rina.org

Certification
T. +39 010 5385703
certification@rina.org