

GDPR



[Link to Impact in CRM presentation](#)
[Link to GDPR Process - Functional Design](#)

General Data Protection Regulation (GDPR)

The General Data Protection Regulation on the protection of natural persons with regard to the processing of personal data and on free movement of such data entered into effect on May 25th, 2018.

Objectives of the law

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data

This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data

The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Key definitions

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

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

Focus - What is personal data ?

"Personal data" is related to an identified or at least identifiable person, called the **"data subject"**

Personal data can have different names:

- personal data
- personal information
- a person's information
- personally identifiable information

Personal data identifies the data subject or make it possible to recognize it:

- **Directly:** surname, first name, photo, professional details...
- **Indirectly:** even by cross-referencing various information making it possible to draw conclusions about the identity of a person: date of birth, postal address, age, diploma, email address, computer IP address, phone number, payment card, license plate number, fingerprint, online behavior, geolocalisation and consumption habits....

An **information** related to a **natural person in his/her workplace** is a **personal data**.

We have different categories of personal data:

- identity data: civil status, identity, identifying information
- personal life: lifestyle, family situation, other than sensitive data
- employment information/professional contact details/business: resume, education, training, competency profile, professional experience, career path within the Group, function, title, department, work place, employment regime, grading, attendance at work, performance appraisals including appraisals, performance reviews and ratings, disciplinary procedure...
- Economic and financial information: income, financial situation, tax status...
- Connection data: IP addresses, access logs...
- Location data: movements, GPS data, mobile data...
- Sensitive information:
 - data revealing political affiliations
 - data revealing religious or philosophical beliefs
 - data revealing trade union memberships
 - genetic information
 - biometric data in order to identify a unique person
 - health data
 - data on sex life and sexual orientation
 - data on criminal convictions and offenses
- Data concerning minors

Scope of Application

GDPR applies to:

- the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
- the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union
 - the monitoring of their behaviour as far as their behaviour takes place within the Union
- the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Rights of the data subject (chapter 3)

Transparent information, communication and modalities for the exercise of the rights of the data subject

- Information to be provided where personal data are collected from the data subject
- Information to be provided where personal data have not been obtained from the data subject
- Right of access by the data subject
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to data portability
- Right to object
- Automated individual decision-making, including profiling

Data collection and processing

The Controller shall collect and process the Personal data according to these principles:

- Lawfulness and fairness Processing
- Consistent purpose
- Data minimisation
- Accuracy
- Time limitation
- Integrity and confidentiality
- Transparency

To comply with the lawfulness and fairness Processing requirement, the Controller shall ensure that at least one of the following applies to qualify the legal basis of the Processing:

- **CONSENT:** the data subject has given consent to the Processing of his or her Personal data for one or more specific purposes
- **PERFORMANCE OF A CONTRACT:** Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps as the request of the data subject prior to entering into a contract
- **LEGAL OBLIGATION:** Processing is necessary for compliance with a legal obligation to which the Controller is subject
- **VITAL INTEREST:** Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- **TASK IN THE PUBLIC INTEREST:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller
- **LEGITIMATE INTEREST:** Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal data, in particular where the data subject is a child.

In case the Processing is legally grounded on the Consent, GDPR requires the Controller to comply with a set of obligations to ensure that the consent is validly obtained.

- 1) why GDPR
- 2) key definitions
- 3) scope of application
- 4) rights of individuals
- 5) Data collection and processing
- 6) Consent