**GDPR**

**What Is the General Data Protection Regulation (GDPR)?**

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in and outside of the European Union (EU). Approved in 2016, the GDPR went into full effect two years later.

The regulation applies regardless of where the data is collected and/or processed, which means it must be heeded by all companies that deal with European citizens, even if they are not EU residents.

Its aim is to give consumers control over their own personal data by holding companies responsible for the way they handle and treat this information.

**To which kind of Data is GDPR applicable:**

* GDPR applies to "information which relates to an identifiable living individual"[[1]](#footnote-1)
* The EU’s GDPR only applies to personal data, which is any piece of information that relates to an identifiable person.
  + The identifiable person is a natural person: This element is the easiest to define. By using “natural person,” the GDPR is saying that data about companies, which are considered “legal persons,” are not personal data.
  + The person must be alive. Data related to the deceased are not considered personal data in most cases under the GDPR.[[2]](#footnote-2)

**How a company is compliant with GDPR regarding its clients:**

To be GDPR compliant, companies must ensure that they are handling personal data in a way that is transparent, secure, and respects the rights of the individuals whose data they are processing. Here are some steps that the company can take to ensure compliance:

* Understand what personal data the company is collecting and processing: This includes information such as names, addresses, email addresses, and other information that can be used to identify an individual.
* Obtain consent from individuals: In most cases, companies must obtain consent from individuals before collecting and processing their personal data. This consent must be freely given, specific, informed, and unambiguous.
* Implement appropriate security measures: Companies must implement security measures to protect personal data from unauthorized access, disclosure, and loss. This includes measures such as encryption, access controls, and regular security audits.
* Appoint a Data Protection Officer (DPO): If your company processes large amounts of personal data or engages in large-scale processing of sensitive personal data, you may be required to appoint a DPO. The DPO is responsible for ensuring that the company is complying with GDPR requirements.
* Develop a Data Protection Policy: Your company should have a clear and comprehensive Data Protection Policy that outlines how personal data is collected, processed, and protected. This policy should be communicated to all employees and regularly reviewed and updated as necessary.
* Ensure compliance with GDPR when transferring data outside of the EU : If your company transfers personal data outside of the EU, you must ensure that the data is being transferred to a country that has adequate data protection laws in place or that appropriate safeguards are in place to protect the data.
* Respond to data subject requests: Individuals have the right to request access to their personal data, request that it be corrected, and request that it be deleted. Your company must have a process in place for handling these requests and responding to them in a timely manner.

**How a third-party processor company is compliant with GDPR regarding its clients?**

By following these steps, the company can ensure that it is GDPR compliant and is handling personal data in a way that respects the rights of individuals and protects their privacy. If the company is a third-party processor, meaning that you are processing personal data on behalf of another company (known as the data controller), then you have additional responsibilities under GDPR.

* In this case, the company must have a written agreement, called a Data Processing Agreement (DPA), with the data controller that outlines the terms of the processing, the nature and purpose of the processing, the type of data being processed, and the security measures in place to protect personal data.
* The DPA should also specify that the company must only process the data for the purposes outlined in the agreement and that you must implement appropriate technical and organizational measures to ensure the security of the personal data. The company must also ensure that the data controller is able to comply with its GDPR obligations, such as responding to data subject requests, and must assist the data controller in meeting its obligations if requested to do so.
* Additionally, if the company is a third-party processor and engages in cross-border processing of personal data, meaning that the personal data is being transferred outside of the EU, it must comply with additional requirements under GDPR. These requirements include ensuring that the data controller has provided appropriate safeguards for the transfer, such as binding corporate rules or standard contractual clauses, and that the transfer complies with any other requirements under GDPR.
* Overall, as a third-party processor, the company must ensure that it is GDPR compliant and is meeting its obligations under GDPR, both in terms of its relationship with the data controller and in terms of any cross-border processing of personal data.

For McKinsey:

On McKinsey's websites it details its [Third Party Sub Processors](https://solutions.mckinsey.com/msd/subprocessors/) and also provides its [McKinsey Data Protection Protocols](https://solutions.mckinsey.com/msd/data-protocols.pdf). If personal data is involved, they must tell the client they work with Infomineo and then list them on their website as Third-Party Sub Processors.

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Timeline

Description automatically generated

1. Information taken from the web site: [UK ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#:~:text=The%20UK%20GDPR%20only%20applies,to%20an%20identifiable%20living%20individual.) [↑](#footnote-ref-1)
2. Information taken from the web site: [EU GDPR](https://gdpr.eu/eu-gdpr-personal-data/) [↑](#footnote-ref-2)