EU GDPR

European General Data Protection Regulation

What is it, and how does it affect your business?

BEIRUTI
Attorneys & Counselors At Law

OVERVIEW

01

“Everyone has the right to respect for his private and family life, his home and his correspondence.”

From this basis, the European Union has sought to ensure the protection of this right through legislation.The GDPR is currently the strictest privacy and security law in the world, imposing obligations onto organisations anywhere in the world, as long as they target or collect data related to people in the EU. Thus, simply put, if a company or organisation processes the personal data of individuals living within the EU, it has to comply with the GDPR regardless of where that company or organisation is based.

Given the rapid development of technology, more people are entrusting their personal data with cloud services, with breaches becoming a daily occurrence. The GDPR puts in place regulations to solidify Europe’s stance on data privacy. The regulation does not use a “one size fits all” approach, and it is quite large, far-reaching and fairly light on specifics, rendering GDPR compliance a difficult matter, particular for small and medium-sized enterprises (SMEs).

Key Definitions

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it’s relatively easy to ID someone from it.

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organising, structuring, storing, using, erasing, etc.

Data subject — The person whose data is processed. These are your customers or site visitors.

Data controller — The person who decides why and how personal data will be processed. If you’re an owner or employee in your organisation who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organisations.

TERRITORIAL SCOPE

02

If you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you even if you're not in the EU.

Territorial scope of the law:

Article 3 GDPR

1. This Regulation 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.

2. This Regulation applies to 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:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to 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.

The offering of goods and services:

The Internet makes goods and services in far-flung places accessible anywhere in the world. The GDPR does not apply to occasional instances. Rather, regulators look for clues to determine whether the organisation set out to offer goods and services to people in the EU. **If your company is not in the EU but you cater to EU customers, then you should strive to be GDPR compliant.**

Monitoring of behaviour:

If your organisation uses web tools that allow you to track cookies or the IP addresses of people who visit your website from EU countries, then you fall under the scope of the GDPR. It however is unclear how strictly this provision will apply.

Exceptions

There are two important exceptions we should note here. First, the GDPR does not apply to "purely personal or household activity." It only applies to organisations engaged in "professional or commercial activity." Second, is for organisations with fewer than 250 employees. Small- and medium-sized enterprises (SMEs) are not totally exempt from the GDPR, but the regulation does free them from record-keeping obligations in most cases (see Article 30.5).

COST OF NON-COMPLIANCE

03

The fines for violating the GDPR are very high.

"***The fines must be effective, proportionate and dissuasive for each individual case.***"

For the decision of whether and what level of penalty can be assessed, the authorities have a statutory catalogue of criteria which it must consider for their decision. Among other things, intentional infringement, a failure to take measures to mitigate the damage which occurred, or lack of collaboration with authorities can increase the penalties.

SEVERE VIOLATIONS UNDER ART. 83(5) GDPR

the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year, whichever is higher.

- the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- the data subjects' rights pursuant to Articles 12 to 22;
- the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- any obligations pursuant to Member State law adopted under Chapter IX;
- non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

LESS SEVERE VIOLATIONS UNDER ART. 83(4) GDPR

sets forth fines of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher.

- the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- the obligations of the certification body pursuant to Articles 42 and 43;
- the obligations of the monitoring body pursuant to Article 41(4).

ART 5. GDPR DATA PROTECTION PRINCIPLES

LAWFUL PROCESSING OF DATA
ARTICLE 6 GDPR

05

Unambiguous Consent

The data subject gave you specific, unambiguous consent to process the data. (e.g. They've opted in to your marketing email list.)

To Enter Into A Contract

Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. (e.g. You need to do a background check before leasing property to a prospective tenant.)

To Comply With a Legal Obligation

You need to process it to comply with a legal obligation of yours. (e.g. You receive an order from the court in your jurisdiction.)

To Save Somebody's Life

Processing of data is necessary to save somebody's life

To Perform a Task in the Public Interest

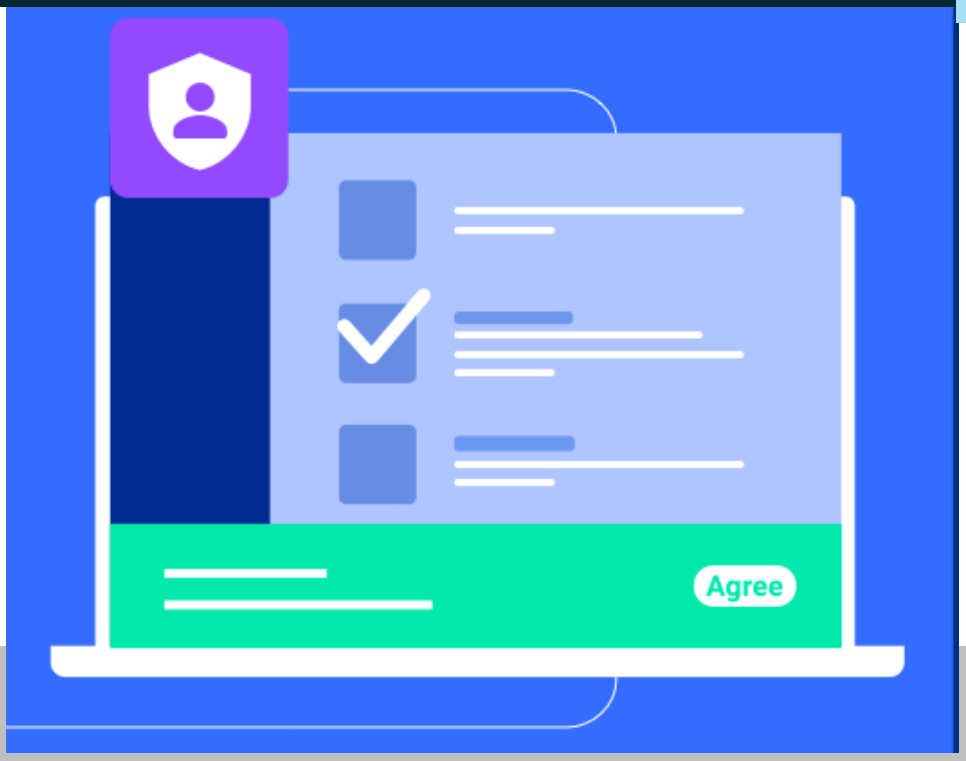
Processing is necessary to perform a task in the public interest or to carry out some official function. (e.g. You're a private garbage collection company.)

Legitimate Interest

You have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data.

CONSENT

06



The GDPR sets out strict rules regarding consent of data subjects to have their data processed.

- Consent must be “freely given, specific, informed and unambiguous.”
- Silence, pre-ticked boxes or inactivity should not therefore constitute consent
- This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data
- Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”
- Data subjects can withdraw previously given consent whenever they want, and you have to honour their decision. You can’t simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent.

Privacy by Design

Any action a company undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the IT department, or any department that processes personal data, must ensure that privacy is built in to a system during the whole life cycle of the system or process. Up to now, tagging security or privacy features on at the end of a long production process would be fairly standard.

Privacy by Default

Once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. If more information than necessary to provide the service is disclosed, then "privacy by default" has been breached.

DATA SUBJECT'S PRIVACY RIGHTS

08

1

The right of Access to information:

1) the right to know whether data concerning him or her are being processed and 2) if so, access it with loads of additional stipulations (GDPR Article 15).

2

The right to rectification:

When personal data are inaccurate, then controllers need to correct them indeed (GDPR Article 16).

3

The right to erasure/ the right to be forgotten:

with additional stipulations, among others if personal data has been made public (GDPR Article 17)

4

Right to restrict processing:
the right of the consumer or whatever you call the natural person under the scope of the GDPR, to limit the processing of his/her personal data with, once more, several rules and exceptions of course (GDPR Article 18).

5

The right to be informed:
the GDPR asks controllers and so on to inform data subjects on several matters. Providing clear and correct information is a key duty in many regards

6

The right to data portability:

the right to transfer personal data from one electronic system to another electronic system

7

The right to object:

data subjects can say they don't want the personal data processing to be done or going on

8

Rights in relation to automated decision making and profiling

GET IN TOUCH

FOR FURTHER INFORMATION, PLEASE DO NOT HESITATE TO CONTACT US

BEIRUTI
Attorneys & Counselors At Law