GOWLING WLG

ARE YOU COMPLIANT WITH THE NEW EU GENERAL DATA PROTECTION REGULATION?

16 April 2018

On May 25, 2018, Regulation (EU) 2016/679 of April 27, 2016, better known as the General Data Protection Regulation ("**GDPR**"), will fully apply in the 28 Member States of the European Union ("**EU**"). A version of the GDPR will have been introduced into Norway's, Iceland's and Lichtenstein's laws so that similar regulations will also apply in these three other countries within the European Economic Area ("**EEA**").

Any activities or practices that do not comply with the GDPR will mean that the organization faces administrative penalties of up to 20,000,000 Euros or, if higher, 4 per cent of the previous financial year's total worldwide annual revenues and even criminal penalties. The offending party may also be held civilly liable for damages caused by non-compliance.

Scope of application for non-European companies

Non-European companies to which the GDPR (or the corresponding law in Norway, Iceland or Lichtenstein) applies are:

- those with an establishment (subsidiary or branch) in an EU (or EEA) country, in respect of all processing of personal data in that establishment (as controller or processor, as defined by the GDPR); and
- those that do not have an establishment in the EU (or EEA), but which are processing (as controller or processor) personal data of natural persons who are in the EU (or EEA) in relation to the offering goods or services to these persons or the monitoring of their behaviour, with regard to such processing activities only.

The GDPR's preamble states that while a website's mere accessibility is insufficient to ascertain the intent to offer goods and services to persons in the EU, "factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union."

Article 28 of the GDPR stipulates that European controllers (and non-European controllers to which the GDPR applies) may only use "processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements" of the GDPR, and those same contractors must sign a contract with such processors containing commitments in that regard. Consequently, non-European companies that wish to sell their services to European companies will naturally implement such measures to avoid being disregarded.

Fundamental principles

For controllers, complying with the GDPR means, above all, ensuring that the personal data concerned is processed according to the following principles, subject to any standards adopted by the supervising authority of the relevant country:

- lawfulness, fairness, transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation;
- integrity and confidentiality;
- accountability.

The principle of lawfulness requires any processing activity to have a legal basis such as: the performance of a contract with the data subject, compliance with a legal obligation, the controller's legitimate interests or-but more rarely, since it can be withdrawn at any time-the consent of the data subject. The legal grounds for processing "sensitive" data or data concerning criminal convictions and offences are more limited.

The accountability principle is new and replaces the a priori control through declarations and authorization requests under the previous rules. The accountability principle requires that "appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met" not only at the time of the processing but also

upon its design (privacy by design and by default).

Records, impact assessments, data protection officer (DPO) and representative

In applying the accountability principle, the GDPR requires companies to keep a record of all their processing activities as controller and, if applicable, a second record of their processing activities as processor. A considerable amount of information needs to be recorded for each processing activity - the purpose of the processing, the categories of recipients, data storage periods, etc. The records may be inspected by the supervisory authorities.

Furthermore, when a type of processing operations is likely to result in a high risk to the rights and freedoms of natural persons, the controller must first assess the impact of the envisaged processing operations on the protection of personal data. Depending on the results of this assessment, a consultation by the supervisory authority may be required prior to processing. The scope of this obligation is specified in guidelines and positions of supervisory authorities in certain countries.

Some companies will need to appoint a data protection officer. This applies to controllers or processors whose core activities involve processing operations that require regular and systematic large-scale monitoring of data subjects or large-scale processing of sensitive data or personal data relating to criminal convictions and offences.

All businesses that do not have an establishment in the EU but are subject to the GDPR must appoint a representative in the EU.

For this purpose, it is recommended that the company be audited. Such audits are usually carried out with (often pre-filled) questionnaires sent to the company's different departments.

Policies

Given the obligation to implement "technical and organizational measures" as a corollary of the accountability principle, it is recommended that companies adopt the following internal policies:

- a general data protection policy;
- a data retention policy;

- a data subject rights handling policy to effectively address (within one month) requests for access, rectification, erasure, restriction of processing and data portability, objections, and to exercise their right not to be subject to a decision based solely on automated processing, given that several of these rights are new (articles 15 to 22 of the GDPR);
- a data breach management policy to manage data breach notices to the supervisory authorities and the data subjects of a personal data breach, according to the GDPR's new provisions in this regard;
- a policy on conducting data protection impact assessments;
- if applicable (mandatory for companies with fewer than 50 employees in France), a procedure for gathering reports from whistle-blowers.

While adequate security measures must also be taken if the company has not already done so, article 32 of the GDPR does not contain any substantively new elements in this regard.

Contracts, notices and consent forms

The GDPR's provisions concerning the transfer of data to countries outside the EEA that did not obtain an adequacy decision from the European Commission are similar to the previous provisions. A company subject to the GDPR must therefore require most of its American partners (more specifically, those not certified "Privacy Shield" and to which no other "appropriate safeguard" applies) to sign agreements containing standard "controller/controller" or "controller/processor" clauses approved by the European Commission.

The GDPR now requires joint controllers (who jointly determine the purposes and means of processing) to contractually define each of their roles as regards the exercising of data subjects' rights and to make the "essence of the arrangement" available to the subjects.

As stated above, the GDPR now requires controllers and processors to sign a contract that defines:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data processed;
- the categories of data subjects;
- the controller's obligations and rights.

This contract must forbid the processor from having recourse to another processor without the controller's prior specific or general authorization, with the controller reserving the right to object to a sub-processor in case of general authorization. It must also impose certain obligations on the processor, including assisting the controller by appropriate technical and organizational measures insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights, and assisting the controller in ensuring compliance with the obligations pursuant to articles 32 to 36 of the GDPR (security, notification of a personal data breach, impact assessments). Existing contracts between a controller and a processor must therefore be amended with effect from May 25, 2018 for the purposes of adding a schedule containing these new provisions.

The GDPR requires controllers to provide data subjects with certain information, part of which did not have to be provided under the previous rules, such as how long the data will be stored, the legal basis of the processing, the data subjects' new rights, etc. It will therefore be necessary to review the data privacy notices and clauses within the general terms and conditions.

When the data processing is based on the data subject's consent, the consent form may need to be reviewed in light of the GDPR's new requirements.

Related Tech, Cyber Security & Data Protection Law

Author

Danhoé Reddy-Girard

Partner - Paris

Email

danhoe.reddy-girard@gowlingwlg.com

Phone

+33 (0)1 42 99 35 45

vCard

Danhoé Reddy-Girard

Are you GDPR compliant?

Take a look at our checklist to make sure you have completed all of the tasks needed in order to comply with the GDPR.