General Data Protection Regulation – Two years on, are you compliant?

March 21, 2021

The EU General Data Protection Regulation came into effect on 25th May, 2018 ("**GDPR**") and is coined as the most comprehensive changes to data protection around the world in the last 20 years. The GDPR rules apply to almost all private sector processing by organizations in the EU or by organizations outside the EU which target EU residents. The maximum fines for non-compliance are the higher of €20m and 4% of an organization's worldwide turnover.

Many organizations state on their websites and represent to their customers that they are GDPR compliant. But what exactly are the practical steps that organizations need to take to meet these legal requirements of the GDPR?

1. Determine whether your organization is subject to GDPR and needs an EU Representative

The GDPR applies to controllers and processors established in the EU and to non-EU establishments "offering goods or services" to or "monitoring" the behavior of persons in the EU. Such non-EU controller or processor within the extra-territorial reach of the GDPR must designate a representative in a Member State in which data subjects are being offered goods and services or behavior monitored unless an exception applies.

2. Determine your organization's Main Establishment

If controllers or processors have establishments in more than one EU Member State, it should determine which of its

establishments is the “main establishment” using the criteria set out in the GDPR and assess which Supervisory Authority is the lead Supervisory Authority that will enforce the GDPR in respect of cross border processing.

3. Data Governance and Accountability

Organizations must implement measures to reduce the risk of non-compliance with the requirements of the GDPR and be able to demonstrate that data protection has significant prominence as well as board attention and support. Data protection officers should report directly to the highest management level within the organization. Large organizations should implement a formal data protection program. A Controller must be able to demonstrate compliance with the obligations on a Controller set out in the GDPR (e.g data protection principles or legal basis for processing personal data).

4. Data Processing Inventory or Article 30 Register

Controllers are required to create and maintain a formal, written record of processing activities under its responsibility except where the Controller employs less than 250 persons and the processing is not likely to result in a risk for the rights and freedoms of data subjects, is not occasional, or is not of special categories of data. Processors are required to record all categories of personal data processing activities carried out on behalf of a controller and to provide a copy to the Controller or a data protection authority on request.

5. Appointing a Data Protection Officer (DPO)

Controllers and Processors must assess whether they are required to appoint a DPO, for example including (a) where its core activities consist of processing operations which require “regular and systematic monitoring” of data subjects on a “large scale”; or (b) where its core activities consist of processing of special categories of data on a “large scale”;

or (c) where required under Member State law. The DPO should report to the highest management level of that organization and should be supported by skilled and appropriate resources. The DPO's contact details must be notified to the Supervisory Authority as the first point of contact in relation to data protection matters.

6. Conducting Data Protection Impact Assessments

Controllers are required to conduct data protection impact assessments where a type of processing is likely to result in a high risk to the rights and freedoms of individuals and is required at least in the following cases:

- a systematic and extensive evaluation of the personal aspects of an individual, including profiling;
- processing of sensitive data on a large scale;
- systematic monitoring of public areas on a large scale.

Data Protection Authorities, in consultation with the European Data Protection Board may provide a white list where a DPIA would be required. The controller may consult with the Data Protection Authority prior to commencing the processing activity regarding any residual risks that cannot be mitigated.

7. Privacy Notice

Organizations are required to provide an information notice to data subjects including the source of the data, the legal basis for processing the personal data, the period for which the personal data will be retained, and the third party recipients of the data. The information duty differs where the personal data has been obtained directly from the data subject or from a third party. Unlike privacy policies that previously sat in website footers, the GDPR requires that the notice must be given in a concise, transparent, intelligible and easily accessible form using clear and plain language. Icons may be used. Where presented electronically the information conveyed

by the icons must be machine-readable.

8. Subject Access Requests

Controllers are required to comply with subject access requests which include:

1. To information about a Controller’s processing (right to be informed)
2. To restrict the processing of personal data (right to object)
3. To request that personal data held by the Controller is rectified were inaccurate (right of rectification)
4. To have a copy of personal data and information (right of access)
5. To have personal data transmitted to the data subject or another controller in a commonly used machine-readable format (data portability)
6. To require the controller to erase personal data in certain circumstances and where the data has been made public to take reasonable steps to inform controllers that are processing the data that the data subject has requested its erasure of any links to, copies or replication of it (right to be forgotten or right of erasure)
7. To object to automated decision making or profiling

9. Data Breach

Organizations are required to notify Data Protection Authorities within 72 hours and data subjects without undue delay in certain high-risk circumstances. A personal data breach register is also required.

10. Data Processing Agreements

Controllers are required to engage processors who provide sufficient guarantees of compliance with the obligations of the GPDR on a processor and must enter into a data processing

agreement meeting the requirements of Article 28.3 of the GDPR.

Is your organization compliant or on the journey towards compliance?

Every organization is unique but there are many milestones that must be achieved before it can say that it is GDPR compliant as part of its data protection compliance program. The fines for non-compliance with GDPR may be up to €20 million, or 4% of the annual worldwide turnover of the preceding financial year, whichever is greater. Is your organization compliant or on the journey towards compliance? If not, create a team led by your legal compliance experts along with HR, commercial, finance, and marketing teams. Implementation of a data protection compliance program will entail more than a simple communication of these concepts to your organization but also the creation of new processes, policies and procedures, training and awareness and ultimately the building of a privacy culture across your business in order to manage data protection risk.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/