COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Does GDPR Apply to My Organization?

By Robert Bond[1]

The European Union (EU) General Data Protection Regulation (GDPR)[2] came into force on May 25, 2018, and continues to have a significant impact upon Legal and Compliance. While the vast majority of companies to which GDPR applies have taken the necessary steps to comply with its requirements, newcomers will want to have a thorough understanding of its scope to determine their exposure.

Applicability

GDPR applies to controllers and processors that have subsidiaries or affiliates in the EU and the UK. A controller is a business that makes decisions in relation to personal data, whereas a processor is a third party that carries out processing on the instructions of the controller.

When the UK left the EU, from the beginning of 2021 the UK has continued to abide by the UK GDPR, which is the same as the EU GDPR. Organizations that have operations in the UK and the EU now have to comply with both legal regimes.[3]

Data Protection Principles

GDPR also has an extraterritorial nature. It applies to any controller or processor that is not located in the EU nor the UK but has processing activities related to either the offering of goods or services to data subjects in the EU or the UK, irrespective of whether a payment is required or not, or where the processing activities relate to the monitoring of the behavior of citizens, so far as that behavior takes place within the EU or the UK.

Many businesses are subject to GDPR whether or not they have entities in either the EU or the UK. If GDPR applies to controllers or processors outside the EU/UK, and if they process large volumes of sensitive data, or if such processing could result in a risk to the rights and freedoms of individuals, then they need to designate in writing a representative who is established in a member state located where data subjects are. When processing of EU or UK citizens' personal data takes place, the representative needs to be appointed in the member state where most of the EU citizens whose data is being processed are located. If the UK is the processing location, the representative has to be appointed in the UK.

The role of the representative is to sit between the controller or processor and the relevant supervisory authority and/or data subjects. The representative will need to respond to investigations or communications from the relevant supervisory authority and/or from data subjects and need to have in place a suitable contract to define roles and responsibilities. The designation of a representative does not affect the primary responsibility and liability of the controller or processor under GDPR.

GDPR lays out data protection principles, which are that personal data must be:

- Processed fairly, lawfully, and in a transparent manner;
- Collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible

with those;

- Adequate, relevant, and limited to what is necessary in relation to the purposes for which personal data is processed;
- Accurate and, where necessary, kept up to date;
- Kept in the form that permits identification of data subjects for no longer than is necessary;
- In accordance with data subjects rights;
- In a way that ensures appropriate security of the personal data; and
- Not transferred to a third country or to an international organisation if the third country has not been deemed to have laws that adequately protect the rights of data subjects.