Assigning Organizational Responsibility for Data Privacy

Applicability

General Data Protection Regulation ("GDPR") allocates specific responsibilities for data protection practices and when a Data Protection Officer ("DPO") is mandatory. Depending on the organizational operations, this may not be the case, compliance responsibility for GDPR may be either allocated to an individual or broadly across the organization. If the controller or processor is not established in the European Union ("EU") and they process personal data of EU citizens or residents, there may be a requirement to have a representative in the EU.

Responsibility Models

If the controller or processor does not have a mandatory obligation to assign a DPO, Recital 62, states that the organization shall assign clear attribution of responsibilities. These data protection requirements can be allocated across the organization, such as Operations and Compliance or other functions; allocated to an existing team within IT, Security, Legal or Risk Management; assigned to a Central Privacy team; or a hybrid model.

When assignment of individual responsibility, either as a DPO or otherwise is required, it does not mean that the functions have to be exclusively managed centrally. The responsibilities can be constructed on any of the models mentioned above, however the allocation of the DPO prerequisites shall follow the requirements laid down in the Regulation.

Controller or Processor not Established in the European Union

When a controller or processor is not established in the EU the GDPR still applies when they are processing personal data of EU data subjects relating to:

- Goods or services offered to them, whether paid or not; and
- Monitoring of their behaviour within the Union.

Designating a Representative

If either or both of these circumstances apply, the controller or processor has to designate, in writing, a representative within the EU or in another region. It should be noted that the designation, whilst mandatory does not remove the possibility of legal action being initiated against the controller or processor themselves.

The representative has to be:

- Able to support and address requests or concerns raised by the data subjects when the goods or services are offered in the EU, or when proofing or monitoring is occurring; and
- Mandated by the controller or processor to be addressed by the Statutory Authorities (SAs) and the data subjects, in addition to, or instead of them. They will therefore need to be in a position to deal with all issues relating to the personal data processing and compliance with the Regulation.

Exception to the Designation of a Representative

This obligation does not apply if the controller or processor is a public authority or body. Or if the processing passes a three part test:

- processing occurs occasional;
- not considered large scale processing of special categories of data (listed below); and
- unlikely to result in a risk to the data subjects rights and freedoms, because of the nature, context, scope and purpose of the processing.

Special Categories of Data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic or biometric data, where identifying an individual
- Health
- Sex life or sexual orientation
- Criminal convictions