BDO

# PRIVACY SERVICES: GDPR

BDO MALTA


# A CUSTOMIZED, PROACTIVE APPROACH.

The European Union (EU) General Data Protection Regulation (GDPR) is far reaching – and is the most rigorous new privacy law in 20 years. The new regulation replaced the Data Protection Directive 95/46/EC and affects organizations in the EU or those that offer goods and services to individuals in the EU, or that collect and analyse data related to EU residents, regardless of their location. This is a complex regulation that impacts nearly all businesses.



# WHAT'S NEW UNDER THE NEW GDPR LAW?

## INCREASED TERRITORIAL SCOPE (EXTRA-TERRITORIAL APPLICABILITY)

GDPR applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

## PENALTIES

Under GDPR, organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' will not be exempt from GDPR enforcement.

## BREACH NOTIFICATION

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

## CONSENT

The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

# WHAT'S NEW UNDER THE NEW GDPR LAW?

CONTINUED

## RIGHT TO ACCESS

The right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

## RIGHT TO BE FORGOTTEN

Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. Includes erasure of data no longer being relevant to original purposes for processing, or a data subject withdrawing consent.

## DATA PORTABILITY

The right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly used and machine-readable format' and have the right to transmit that data to another controller.

## PRIVACY BY DESIGN

Calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. 'The controller shall… implement appropriate technical and organisational measures… in an effective way…in order to meet the requirements of this Regulation and protect the rights of data subjects'.

## DATA PROTECTION OFFICERS (DPO)

DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.



# SUPPORTING OUR CLIENTS THROUGH THE GDPR PROCESS

At BDO, our team of experienced professionals is dedicated to helping our clients succeed. We start by helping them understand their GDPR compliance obligations, before creating and executing a remediation plan designed to minimize cost and disruption while meeting all requirements. While every plan is specifically customized to meet each of our clients' unique situations, our main services are aligned to support the most common GDPR compliance requirements, including:

## GDPR READINESS

- GDPR readiness assessment;
- Data mapping / data flow diagramming;
- Article 30 register development and management;
- Article 6(1) and 9(1) information audit and inventory
- Incident response planning and testing;
- Data protection impact assessments (DPIA)/ privacy impact assessments (PIA);
- Information security assessments;
- Privacy program advisory.

## OUTSOURCED / VIRTUAL DATA PROTECTION OFFICER (DPO) SERVICES (ARTICLES 37-39)

- Development and business alignment;
- Setup and configuration;
- DPO Support.

## REMEDIATION AND IMPLEMENTATION

- Data minimization, retention, erasure and classification policies and process development;
- Training and awareness;
- Privacy internal campaigns;
- Privacy notices, policies and procedures development;
- Privacy by design and default;
- Technical controls implementation;
- Third-party processor remediation;
- Review privacy agreements / clauses;
- Data breach response and notification process planning;
- International data transfers policies and registers development.

FOR MORE INFORMATION:

**BDO MALTA**

Triq it-Torri Msida
MSD 1824
Malta

Tel: +356 2342 4000

info@bdo.com.mt



**www.bdo.com.mt**