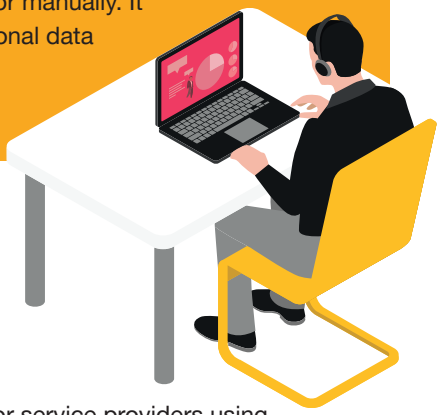
General Data Protection Regulation

Where are you on your GDPR journey?

GDPR at a glance

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. The objective behind this european regulation was to modernise laws due to rapid technological changes in order to protect individuals personal information and to harmonise data privacy laws across Europe. The GDPR gives greater protection and control to individuals over their information and transforms the way organisations handle information from their customers and employees.

Processing of data covers anything one does with personal data, including holding or storing it either electronically or manually. It is essential that any business that processes personal data about EU citizens complies with the GDPR.



How does it impact your business?

The GDPR outlines six principles that companies or service providers using customers' personal data must follow for **good data protection practice**, namely:

1 Lawfulness, fairness and transparency

When collecting data, organisations must ensure that the processing is legitimate. Data subjects have a right to know how and why their data is being collected and used. This ensures a good company-customer relationship and reduces the risk of complaints and/or requests from data subjects.

2 Purpose limitation

Any organisation must ensure that data is collected for 'specified, explicit and legitimate' purposes, limiting processing to the data required and therefore, data collected for one purpose may not be used also for a totally different purpose.

3 Data minimisation

The principle of minimisation requires businesses to make sure that the data processed for a specific purpose is kept to the minimum. Ensuring that processed data is not excessive reduces the risk of complaints by data subjects whilst limiting the need to carry out further exercises to get rid of unnecessary data.

4 Accuracy

The GDPR stresses that organisations are obliged to ensure that any data which is inaccurate or incomplete is either set right or destroyed. Data subjects may also request to have their data revised whilst organisations must ensure to make ends meet with such demands without any unnecessary delay.

5 Storage limitation

Having adequate retention policies and disposal mechanisms in place facilitates the smooth running of the business while ensuring compliance. Storage of data, even in archives, constitutes data processing. This means that data subjects' rights and controllers' obligations remain applicable even when the business stops to actively make use of the data.

6 Integrity and confidentiality

Organisations must ensure that data collected is secured in order to ensure lawful and authorised processing, while protecting against accidental loss, destruction or disclosure. Therefore, organisations must use appropriate 'technical or organisational measures'. Unsecure data can cause immense damage to an organisation if data is stolen or disclosed to third parties. A data breach leads to considerable obligations to investigate, report and remediate. It may also result in significant penalties.

How can we help

Your organisation may be just getting started - or may already have a GDPR programme in place. We can help you make the best of this regulation, regardless of where you are on your GDPR journey. Here is how our team can help you with:

Data Protection Audits

- Reviewing internal processes and procedures
- Reporting an implementation plan of action
- Assistance and support in carrying out the recommended plan of action

Provision of customised data protection training sessions

- Data protection awareness sessions for new staff members
- Data protection management sessions tailored according to the roles and industry
- Periodical awareness sessions and refresher training
- Training sessions specifically tailored for the staff members carrying out the DPO role

Outsourcing or co-sourcing of DPO role

- Ad hoc support to acting DPO's
- DPO outsourcing services
- Outsourcing of specific DPO functions
- Assistance in the development, implementation and compliance with policies and procedures relating to data protection
- Assistance and guidance in the maintenance of a proper register of processing operations
- Monitoring compliance with the GDPR and other applicable data protection laws through data protection audits.

- Cooperating and liaising with the Maltese Commissioner and with other data protection authorities and to act as the point of contact for the Maltese Commissioner on issues related to the processing of personal data, including; facilitating the supervisory authority's access to documents and information for the purposes of carrying out its investigative, corrective, authoritative and advisory powers and the DPO may also seek advice from the authority on certain matters when appropriate.
- Provide guidance on data protection matters relating to data subjects including subject access requests.
- Provide support management in a case of data breach or incidents relating to personal data, including guidance on the notification and communication with the data protection authorities and, where necessary, to the data subjects and other authorities.

Data Protection Assessments

- Data Protection Risk Assessments
- Data Protection Impact Assessments

Incident management readiness

- Assessment of incident and breach management procedures in place
- Breach assessment simulation exercise
- Assistance with implementation of procedures

Incident management support

- Triage and impact assessment
- Communication (internal; Data Protection Authorities; data subjects)
- Reporting

Contact us

Mark Lautier
Tax Partner, PwC Malta
E: mark.lautier@pwc.com
T: +356 2564 6744

Follow us on: