VGDA
AUDIT – TAX – ADVISORY

Preparing to comply with GDPR

26 February 2018

Background Overview

The General Data Protection Regulation ("GDPR") has been approved by the EU Parliament on 14 April 2016 and its entering into force as from ***25 May 2018***. After this time those organisations which will be found non-compliant may face heavy fines.
In case your Company is collecting, managing and processing personal data, this document aims to inform on how you might be affected by the main provisions of this new regulation.

What is GDPR?

The GDPR replaces the Data Protection Directive 95/46/EC and aims to harmonise and update current data protection laws across the EU. The impending changes will impose stricter fines on companies mismanaging personal data or failing to protect it properly.

The GDPR is based on the principle of good data governance. At the heart is the idea of privacy being a fundamental right. For this to be achieved, it's organisations must insist on "privacy by design", "privacy by default" and "accountability".

Who is affected?

The GDPR has a broad territorial scope. It applies not only to all organisations established in the EU that process personal data, but also to any non-EU established organisation that process personal data of individuals who are in the EU in order to:

a. offer them goods or services, irrespective of whether a payment is required; and
b. monitor their behavior within the EU.

The GDPR's aim is to protect personal data at all stages of data processing. The GDPR identifies two different entities that both have obligations: data controllers and data processors.

What are Data Controllers and Data Processors?

A *data controller* is the entity that determines the purposes, conditions and means of the processing of personal data. For example, educational and research private and public institutions, healthcare services, or any business that manages the personal data of their employees and customers.

A *data processor* is an entity which processes personal data on behalf of the controller, such as a cloud provider (for example a Software-as-a-Service like CRM software). It is important, that a company can act both as a controller and processor, depending on the exact type and usage of data.

What are the Sanctions and Liabilities for Non-Compliance?

Data controllers and data processors face severe consequences if they do not comply with the European rules. Depending on the infringed provision of the GDPR, fines may amount to a maximum of €20 million or 4% of global annual turnover of the controller, whichever is higher. Moreover, both controller and processors are subject to joint liability for damages.

The GDPR also gives individuals the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR. In certain cases, not-for-profit bodies can bring representative action on behalf of individuals. This opens the door for mass claims in case of large-scale infringements.

Key Provisions (1 of 2)

Data Protection Principles

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

Accountability and Governance

You must be able to demonstrate compliance with the GDPR:

- The establishment of a governance structure with roles and responsibilities.
- Keeping a detailed record of all data processing operations.
- The documentation of data protection policies and procedures (Manual).
- Data protection impact assessments (DPIAs) for high-risk processing operations.
- Implementing appropriate measures to secure personal data.
- Staff training and awareness.
- Where necessary, appoint a data protection officer.

Data Protection by Design and by Default

There is a requirement to build effective data protection practices and safeguards from the very beginning of all processing:

- Data protection must be considered at the design stage of any new process, system or technology.
- A DPIA is an integral part of privacy by design.
- The default collection mode must be to gather only the personal data that is necessary for a specific purpose.

Valid Consent

There are stricter rules for obtaining consent:

- Consent must be freely given, specific, informed and unambiguous.
- A request for consent must be intelligible and in clear, plain language.
- Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
- Consent can be withdrawn at any time.
- Consent for online services for a child (defined between the age of 13 to 16) is only valid with parental authorisation.
- Organisations must be able to evidence consent.

Key Provisions (2 of 2)

Privacy Rights of Individuals

Individuals' rights are enhanced and extended in a number of important areas:

- The right of access to personal data through subject access requests.
- The right to correct inaccurate personal data.
- The right in certain cases to have personal data erased ("right to be forgotten").
- The right to object.
- The right to move personal data from one service provider to another (data portability).

Transparency and Privacy Notices

Organisations must be clear and transparent about how personal data is going to be processed, by whom and why.

- Privacy notices must be provided in a concise, transparent and easily accessible form, using clear and plain language.

Data Transfers Outside the EU

The transfer of personal data outside the EU is only allowed:

- Where the EU has designated a country as providing an adequate level of data protection;
- Through model contracts or binding corporate rules; or
- By complying with an approved certification mechanism, e.g. EU-US Privacy Shield.
- Any transfer outside the EU that does not fall under the above circumstances could lead to personal liability to the Company and fines.

Data Security and Breach Reporting

Personal data needs to be secured against unauthorised processing and against accidental loss, destruction or damage.

- Data breaches must be reported to the data protection authority within 72 hours of discovery.
- Individuals impacted should be told where there exists a high risk to their rights and freedoms, e.g. identity theft, personal safety.

Data Protection Officer ("DPO")

The appointment of a DPO is mandatory for:

- Public authorities;
- Organisations involved in high-risk processing; and
- Organisations processing special categories of data.

A DPO has the following set of tasks:

- Inform and advise the organisation of its obligations.
- Monitor compliance, including awareness raising, staff training and audits.
- Cooperate with data protection authorities and act as a contact point.

Our Services (1 of 2)

GDPR Health Check & Compliance Assessment

A quick assessment to identify the organisation's GDPR exposure. This is the starting point of the process and Indicative services include:

- Quick Gap Analysis offered to clients in order provide readiness rate and help organizations decide whether they need further assessment or not
- Consultation and recommendation of IT tools that will assist will the implementation

We then move forward to conduct a more in-depth compliance assessment. The thorough Data Privacy Impact Assessment is performed whereby all systems (and their interfaces) that store, handle, and process personal data need to be identified, mapped, and documented.

A detailed report is prepared describing the identified processes and systems, as well as guidelines for continuous monitoring of these.

Data Mapping

The process aims to highlight any deviations (compliance gaps) between the desired and actual level of compliance against GDPR.

For each identified deviation, the proposed remediation actions will be listed and these will form the base for the compliance mapping thereon.

GDPR Compliance Framework & Implementation

Further to the detailed GDPR Compliance Gap & Assessment, the detailed activities of the roadmap implementation need to be specified.

An indicative list of the consulting and support services that can be offered, include the following:

- Thorough Gap Analysis and Assessment including Data Privacy Impact Assessment (DPIA)
- Operational implementation of GDPR requirements based on performed Gap Analysis
- Contractual Management review and update (employees, vendors, third party collaborators etc.)
- Consent Forms review and update where applicable

Our Services (2 of 2)

GDPR Training and Awareness & On Demand Services

As required by GDPR, the organization needs to provide general awareness to all personnel as well as specific training to people that handle data. We offer:

- GDPR training and awareness programs (staff awareness)
- GDPR requirements and personal obligations for Data Handlers Training

We further demonstrate flexibility for our customers and support them on ad-hoc privacy matters and specific cases which require handling or consultation. Indicative services may include:

- Contracts Privacy Assessment
- Privacy Case Assessment and Support

Data Protection Policy Manual

- Policies and Procedures design and development for Implementation
- Creation of Manual based on best practices and created processes and controls.

Outsourced DPO Services

In line with the requirements of Article 37 of GDPR, the appointment of a Data Protection Officer (DPO) is required in cases where sensitive data is maintained or the size and complexity of the operation warrants it.

A qualified person from our team functions as the DPO for your organisation providing support on all related issues and acting as the contact person for the supervisory authorities.

In order to facilitate the design of a holistic plan and for the purposes of achieving a smooth and effective implementation, we can consult and coordinate with your internal/external Legal and IT functions. Alternatively, we can identify and suggest to you persons/firms carrying such disciplines and possessing relevant credentials with whom we can cooperate in delivering the required result.

Nicosia Office
32, John Kennedy Avenue
Dadlaw Business Centre, 2nd Floor
1087 Nicosia, Cyprus
Tel.: +357 22 300900
Fax: +357 22 300901

Limassol Office
8, John Kennedy Street
Iris House, 8th Floor
3106 Limassol, Cyprus
Tel.: +357 25 760500
Fax: +357 25 760501

info@vgda.com.cy
www.vgda.com.cy

For more information you may contact:

Vasilis Koufaris
Managing Director
Tel. ☎: +357 99 432000
Email ✉: vkoufaris@vgda.com.cy

Antonis Antoniou
Director, Head of Audit
Tel. ☎: +357 99 699664
Email ✉: aantoniou@vgda.com.cy

Constantinos Christodoulou
Director, Head of Advisory
Tel. ☎: +357 99 657028
Email ✉: cchristodoulou@vgda.com.cy

It is noted that the information contained in this document is of a general nature and is, therefore, not intended to address the circumstances of a particular natural person or legal entity. Whilst the information contained herein has been prepared in good faith, no representation, undertaking or warranty, expressed or implied, is given or will be made and no liability is accepted by VGDA as to the accuracy, reliability, adequacy or completeness of the information contained in this document. No one should act upon such information without appropriate professional advice and after a thorough examination of the particular situation.

VGDA would be pleased to advise recipients of this document on how to apply the principles set out herein to their specific circumstances and requirements.