G.C.Hadjikyprianou & Associates LLC
ADVOCATES & LEGAL CONSULTANTS

GDPR: Key Elements and Steps Towards Compliance

General Data Protection Regulation: An Introduction

The EU General Data Protection Regulation (the "GDPR") came into force on 25 May 2018 and introduced a new intra-union legal framework for privacy and data protection. The GDPR replaced the 1995 Data Protection Directive, which had been transposed into each EU member state's national legislation. While the GDPR resembles the principles of the 1995 Data Protection Directive, it has some important new key elements.

In this brochure, we have summarized some of the key elements and core principles of the regulation and have prepared a high-level step plan that a corporate entity should follow in order to comply with the provisions of the regulation.

KEY NEW ELEMENTS

- Penalties for non-compliance: Up to 20 million euros or 4% of the company's global annual turnover.
- Extended territorial effect.
- Broader definition of "personal data".
- New rights for data subjects, such as 'the right to erase' and 'data portability right'.
- Security & Data breach notifications.
- Data Protection Impact Assessments (DPIAs).
- 'Consent' is now subject to further conditions.
- Strict conditions for international data transfers.
- Strict requirements for data processors engagement.
- New obligations to data controllers and processors.
- Privacy notices: additional information requirements.
- Extended transparency requirements towards data subjects.
- Accountability: requirement to demonstrate compliance with the GDPR throughout the entire data lifecycle.
- Co-operation of data protection authorities (DPAs) to ensure compliance throughout the union.

Extended territorial effect: Applicability to companies outside the EU

The provisions of the regulation apply now to non-EU organisations that offer goods or services to data subjects or monitor behaviour of data subjects within the Union.

The GDPR's principles for processing personal data

The GDPR relies on the following core principles which an organisation should always abide by when processing personal data.

- Lawful; fair and transparent processing
- Explicit and legitimate purpose for processing
- Necessity – Data minimization
- Limitation of storage
- Security and confidentiality
- Accountability

Lawful; fair and transparent processing

Processing should be lawful and fair, and it should be transparent to the data subject.

Explicit and legitimate purpose

Purposes for which data are collected and processed should be explicit and legitimate.

Necessity – Data minimization

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the personal data are processed.

Limitation of storage

The period for which personal data is stored is limited to a strict minimum.

Security and confidentiality

Appropriate measures shall be taken to protect personal data against unauthorised or unlawful processing in order to ensure security and confidentiality.

Accountability

Adopt policies and implement appropriate measures to ensure personal data is secured throughout the entire data lifecycle

"The data protection and privacy regulatory landscape can appear overwhelming to a business of any size. Related compliance failures can give rise to significant reputational damage; substantial regulatory fines; claims for damages as well as loss of corporate value. Thus, data protection and privacy compliance constitutes one of the key risk avoidance strategies for companies today.

Road to GDPR compliance

The GDPR describes how organisations should comply with its principles. The below are the key steps that a corporate entity should follow in order to comply with the provisions of the regulation.

1

Impact Assessment

Companies may be required to execute a comprehensive impact assessment (DPIAs) prior to the processing of personal data where there is a 'high risk' processing activity. DPIAs enable companies to identify possible privacy risks and take measures to eliminate or mitigate the same.

2

Data Mapping

Companies must identify the flow of personal data within, to and from their businesses by documenting every process and procedure in order to have an overview of the data processing activities within their structure.

3

Data processing register

Subject to certain conditions, the GDPR requires most of the companies to maintain a data processing register and keep a track of all the related processing activities.

4

Data retention periods

Companies must also determine the period for which they retain personal data. Personal data should only be retained for as long as necessary for the purposes for which such data have been provided and/or disclosed to the company. Even though this appears to be a very easy exercise, most companies fail to comply with the provisions of the regulation in relation to the retention period.

5

GDPR related agreements with third parties

Whether companies are acting as data processors or data controllers, the regulation requires them to update their related contractual and operational relations with third parties by executing written agreements containing specific data protection provisions.

6

Data breach protocol

Companies are also required to establish an adequate privacy governance structure and in particular to create an effective data breach procedure (detect – investigate – report). The regulation requires organisations to report personal data breaches to the competent authority within 72 hours following the discovery of such a breach.

7

Remediate identified gaps

Companies are obliged to update their policies and procedures and bring them in line with the provisions of the regulation. Amongst the said obligations are the requirement to inform data subjects (eg employees, customers etc) on the processing of their data and obtain their consent before proceeding with any processing activity. The regulation sets out an extensive list of information that must me provided to data subjects and in addition provides a strict definition as to what qualifies as an 'adequate consent'.

8

Data Protection Officers

Subject to certain conditions, companies may be required to appoint a Data Protection Officer – a person responsible to monitor the data related activities of the organisation

9

Security measures

The regulation requires companies to implement adequate security measures and mechanisms to ensure the protection of personal data. Amongst others, companies must take technical and organisational measures in order to be in a position to effectively and efficiently respond to data subject requests.

10

BCRs

Subject to certain conditions, companies may be required to set up Binding Corporate Rules (global code of practice based on EU privacy standards) as a basis for a safe data transfer.

11

Establish lead supervisory authority

Companies operating in more than one EU member state or engaging in cross-border processing activities, shall determine their lead supervisory authority for their group. Any report and/or other required communication shall then be made to the said leading supervisory authority.

Get in touch

Our firm helps our clients to navigate this increasingly complex and highly regulated landscape by providing clear and practical legal advice on data protection and privacy law issues. Our services in this area include, undertaking full General Data Protection Regulation (GDPR) compliance programmes; preparing data processing and data transfer agreements; advising on data sharing and exploitation; advising on cyber security breaches; developing and implementing internal privacy and cookies policies; advising on the privacy aspects of insourcing and outsourcing of business activities; supporting and advising our clients' Data Protection Officers (DPOs) or offering fully fledged DPO services as well as delivering related training programmes for organizations, aiming to create data protection culture amongst their staff and management team. We also frequently undertake related compliance audits within the context of a wider transaction/reorganization such as mergers and acquisitions.

Should you have any questions on issues reported herein or require any related legal advice, please do not hesitate to contact us using the contact details provided hereunder.

G.C.Hadjikyprianou & Associates LLC

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 99908081 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com