

General Data Protection Regulation (GDPR)



The EU General Data
Protection Regulation (GDPR)

 **ELIAS**
NEOCLEOUS
& Co LLC

What is the GDPR?

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) was adopted on 27 April, 2016 to strengthen and unify data protection for all individuals within the European Union. The GDPR entered into full effect on 25 May 2018, and has replaced Directive 95/46/EC. Unlike the Directive, it does not require domestic legislation to implement it, but applies directly throughout the EU.

The main aim of the GDPR is to strengthen and increase the level of control and security over the information stored and processed by an organization. Furthermore, the regulation ensures that data controllers and processors are safe custodians of the data.

The GDPR introduces a number of features, including:

- Obligations on organisations including appointing a Data Protection Officer (DPO) and adopting security policies and procedures
- Obligations to report personal data breaches
- The “One-stop shop”
- Enhancing the rights of data subjects and strengthening rules on minors, social networking activities

The aim of the GDPR is to protect all EU citizens from privacy and data breaches

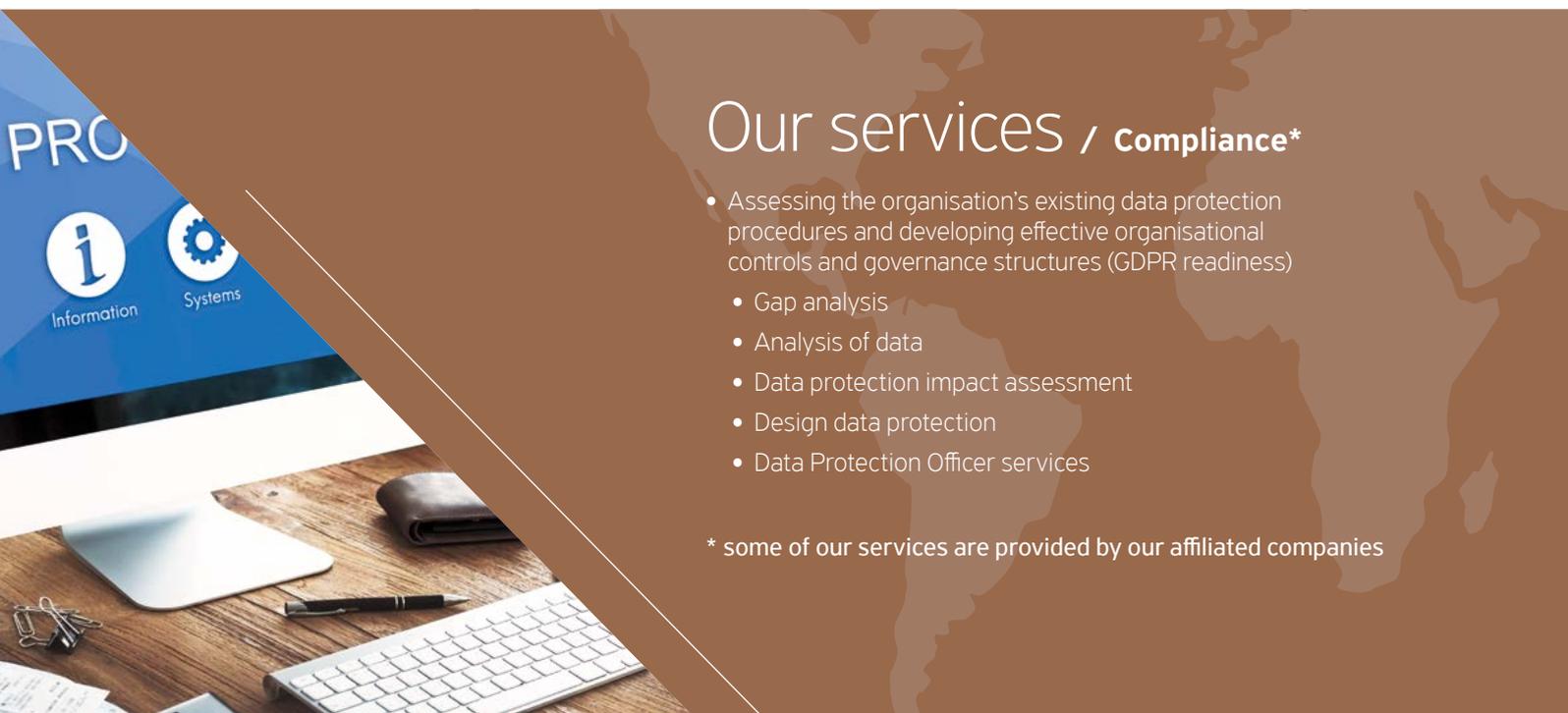
GDPR fundamentally changes the way organizations must manage their people, policies, processes and technology

While data processors have a variety of business models, from on-premises processors to cloud service providers, the provisions which apply to them in respect of the processing of client personal data are the same. The GDPR brought in significant changes, one of which is the direct obligation on data processors for the first time at EU-wide level, enabling data subjects to enforce their rights directly against data processors and apply an enforcement regime which lays the non-compliant data processor open to sanctions, including substantial fines.

Our services / Compliance*

- Assessing the organisation's existing data protection procedures and developing effective organisational controls and governance structures (GDPR readiness)
 - Gap analysis
 - Analysis of data
 - Data protection impact assessment
 - Design data protection
 - Data Protection Officer services

* some of our services are provided by our affiliated companies



Key changes introduced by the GDPR include:

Updated “Personal Data” Definition

Personal Data - “means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

The GDPR adopts a broader definition of personal data than the Directive, which takes into account the increasing use of the internet, bringing more types of data within the scope of the regulation.

Data Protection Officer (DPO)

The appointment of a DPO is mandatory for certain companies. The role of the DPO is designated in certain circumstances by the data controllers and processors in order to ensure compliance with their accountability program and the data protection impact assessment.

If your business is not in the EU, you may still have to comply with the regulation

Consent

The rules for obtaining valid consent have changed. Obtaining consent to process personal data is more difficult to achieve and to evidence. Also, a topic of huge debate relates to parental consent being required for children to receive information society services. The compromise (that Member States can lower the age from 16 to 13) may result in a lack of harmonisation.

One-stop shop

The GDPR introduces the principle of a “one-stop shop”. This means that controllers have to deal only with a single supervisory authority, the authority of the member state where a controller has its main establishment, instead of each of the other EU member states where the controller may also be established. This reduces the administrative burden, uncertainty and inconsistency for data controllers that existed under the previous Directive and benefits on service providers with offices in more than one EU member state.

Our services / Compliance*

- Carrying out a privacy impact assessment for your organisation, as required under the Regulation, to evaluate the nature and sensitivity of the data processing operations you currently carry out or envisage carrying out in the future
- Managing data security breaches
- Monitoring regulatory developments and providing practical impact assessments
- Supporting privacy by design in new projects through adoption of effective tools, instruments or applications

The GDPR is a regulation and applies in its entirety across the EU

* some of our services are provided by our affiliated companies

Right to be forgotten

Subject to certain specified conditions, data subjects have the right to require controllers to erase personal data concerning them without undue delay. A controller who has made the personal data public should also inform other controllers who are processing such personal data to erase any links to, or copies or replications of, those personal data.

If your business is not in the EU, you still have to comply with the GDPR

Non-EU entities which carry out business in the EU with EU data subjects' personal data must comply with the GDPR.

Data breach and consequences

In the event of a personal data breach, the controller must notify the breach to the competent supervisory authority within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it must be accompanied by an explanation of the reasons for the delay.

Introduction of new compliance measures

Mandatory data protection impact assessments have been introduced, which require the undertaking of a risk-based approach prior to carrying out higher-risk data processing activities. Such activities include a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, processing on a large scale of so called "sensitive data", or of certain personal data relating to criminal convictions and offences and systematic monitoring of a publicly accessible areas.

Our services / Legal

- Advising on supply chain and cross-border data issues
- Liaising with the Data Protection Commissioner and other regulators on behalf of the client
- Representing the client in relation to data protection matters before the Data Protection Commissioner and the courts
- Filing Notifications and Applications for Transmission Licenses with the Data Protection Commissioner
- Providing clients with legal opinions in relation to data protection matters such as data transfers to non-EU countries as well as opinions in relation to interpretation of the law
- Drafting Binding Corporate Rules and Model Clauses in accordance with the needs and requirements of the client
- Defending privacy law suits
- Advising on how to maximise value from data assets consistent with the regulatory landscape



Data protection by design

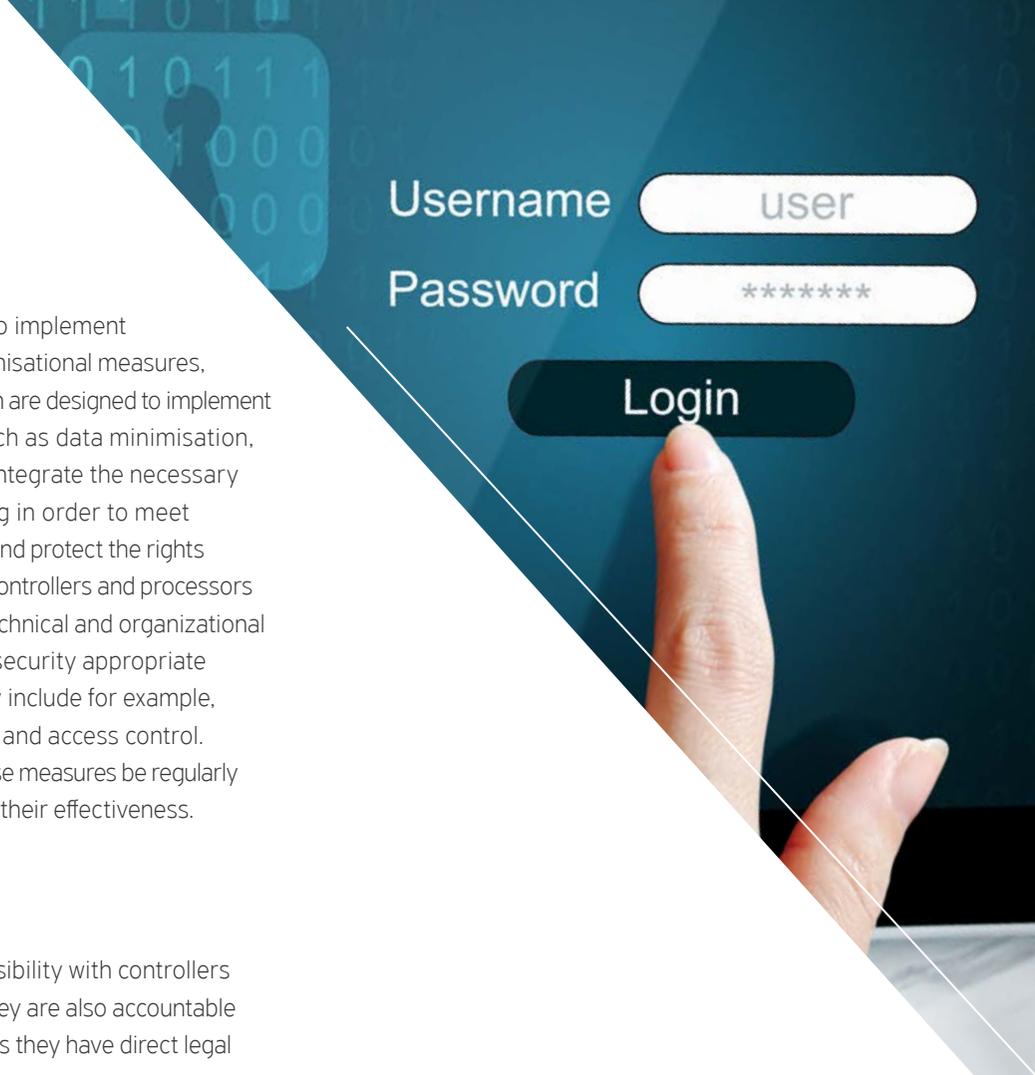
Data controllers are required to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. Furthermore, controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Such measures may include for example, pseudonymisation, encryption and access control. The GDPR also requires that these measures be regularly tested and evaluated to ensure their effectiveness.

Accountability

Data processors share responsibility with controllers for protecting personal data. They are also accountable to individuals under the GDPR as they have direct legal obligations and responsibilities.

Penalties

Substantial penalties are introduced for breach of the GDPR. Organizations found in breach of the GDPR can expect administrative fines of up to 4% of annual global turnover or €20 million - whichever is greater.



Username

Password

Login

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 million

GDPR applies to all enterprises processing and holding the personal data of data subjects residing in the European Union, regardless of the enterprise's location

Building
on our heritage.
Innovating
for the future.

Contact Our Team

gdpr@neo.law

Elias Neocleous & Co LLC is the largest law firm in Cyprus and is internationally recognised as a leading law firm in the South-East Mediterranean region.

We are the only Cyprus firm selected for Legal Business magazine's **"Euro Elite" top 100 firms** in Europe. We have more than 140 fee-earners and a management team whose skills we leverage to assist clients. We serve clients out of three offices in Cyprus and out of an international network of offices in the main destinations for investment via Cyprus.

Our staff have unmatched experience in assisting clients in cross-border investment projects in Europe, Asia, Africa and the Americas. Our attention to client service is what sets us apart.

For us the client comes first.

LIMASSOL

Neocleous House
195 Makarios III Avenue
P.O.Box 50613
CY-3608 Limassol, Cyprus

T: +357 25110110
F: +357 25110001

NICOSIA

5 Lemesou Avenue
2nd Floor
P.O.Box 26821
CY-1648 Nicosia, Cyprus

T: +357 22110300
F: +357 22110001

PAPHOS

S.P. Business Centre
4th Floor, Offices 410-411
17 Neophytos Nikolaidis Ave. & Kilkis
P.O.Box 61297, CY-8132 Paphos, Cyprus

T: +357 26110390
F: +357 26110001



www.neo.law / gdpr@neo.law

This content is for general information purposes only. It is not meant as a legal advice on any transaction and appropriate legal advice should be sought. Elias Neocleous & Co LLC. September 2018. All rights reserved ©.

