The EU GDPR:

New challenges and opportunities in data privacy

ODYSSEY
Impossible Challenges, Possible Solutions

GDPR enforcement goes into effect in May 2018. Are you ready? If you're like most organizations, the answer is probably **"No"**. Get prepared and plan ahead to protect your sensitive data against targeted attacks and breaches ensuring data privacy - or take the risk and pay the price.

What is the EU GDPR

The **General Data Protection Regulation** (GDPR) (Regulation EU 2016/679) was adopted by the European Council and the European Commission on April 27th, 2016 and will be going into full effect on May 25th, 2018. The intended purpose of the Regulation is to strengthen and unify **data protection** for all individuals within the European Union (EU) while giving them better control over their personal data.

Mandatory for all EU Member States and regardless of national legislation, the GDPR binds public and private organizations significantly increasing their compliance obligations with respect to privacy. Non-compliance is punishable with punitive fines high enough to bring this matter at the top of the corporate agenda.

Where it applies

GDPR applies to any organization of any size, even if they are located outside of the EU, as long as they are **collecting, storing and/or processing** personal data of EU citizens.

What it requires

With new obligations on data subject consent, data anonymization and transparency, privacy by design and by default, the GDPR requires organizations which process EU citizens' data to undertake major operational reforms in regards to several factors:

- Processing of personal data throughout their lifecycle, from collection to destruction
- Transferability to other countries
- Protection of individuals' rights
- Security (confidentiality, integrity, availability) of personal data
- Breach notification in case of violation
- Appointment of data protection officers

Penalties for non-compliance

The GDPR is making security an absolute requirement for organizations of any size processing EU citizens' data. Serious infringements will be penalized by fines of up to either €20 million or 4% of total annual worldwide turnover, whichever is higher. Fines are determined by the nature and severity of the infringement.

Challenges for organizations

- The exact knowledge of what data is collected, where it is stored and why it is processed
- Careful assessment of the data collected to ensure appropriate processing e.g. pseudonimization (masking)
- Defining and segregating business needs to ensure that required consent is appropriately collected
- Taking cost-effective measures to reduce the risk of GDPR violations without jeopardizing operational priorities
- Implementation of a Data Protection Framework within the organization which enforces appropriate governance and facilitates the identification and implementation of privacy by design and by default opportunities.

"...the controller and the processor shall implement appropriate...measures to ensure a level of security appropriate to the risk, including...the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

GDPR, Article 32

How We Can Help You

We are proud of our uniquely qualified blend of compliance professionals, data protection experts, and information security specialists whose collective knowledge, experience and expertise can address both the legal/compliance as well as the technical challenges of GDPR enforcement. By employing a holistic approach and possessing ground experience in all the major industries, we can help you address the challenges the GDPR presents.

At the center of these challenges is effective privacy management throughout the entire lifecycle of organizational data. Odyssey explains and maps the appropriate data protection measures at each lifecycle stage.

www.odysseycs.com/GDPR

Data Lifecycle

When it comes to data, the questions are simple. Your organization needs to be constantly and precisely aware of the **who, what, where, when and how.** This begins and ends with a thorough understanding and implementation of the **Data Lifecycle.**

CREATE - The need for data security and privacy begins at the point of data creation and collection. As soon as data is created or altered, organizations need to understand **who is responsible** for that data (information owner) and that there are ways to protect it.

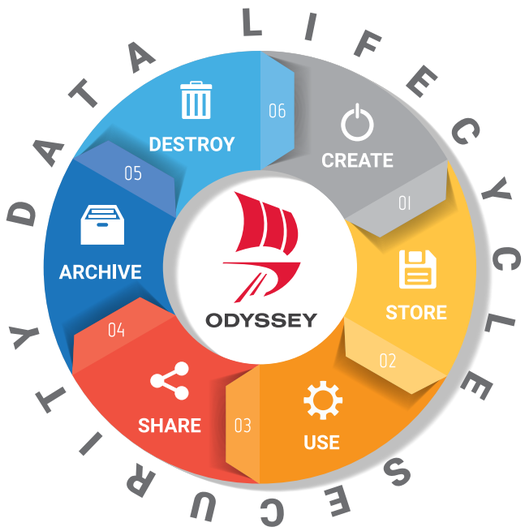
STORE - As soon as data is created, it becomes the organization's responsibility to store it securely and safeguard it against any type of harm, restricting access to those who are unauthorized.

USE - By the time data is stored and is at rest, it becomes usable and can be viewed, copied and altered. At this phase, data is exposed to malicious attacks, unintentional mistakes, unauthorised access and misuse.

SHARE - Data and metadata are constantly travelling and shared among employees and organizations, making it a real challenge to control where data moves through, when on the wire (in transit).

ARCHIVE - At some point of the data lifecycle, data is no longer usable but may still be of value to the organization.

DESTROY - Data marked for destruction continues to bear a value and relevant accountability to the organization, especially if the destruction is legally prescribed, as the case of personal and health information may be.



"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss."

GDPR, Article 5

ODYSSEY'S SERVICES & PRODUCTS	CREATE	STORE	USE	SHARE	ARCHIVE	DESTROY
Data Discovery and Classification	√	√	√	√		
ISO 27001 Implementation	√	√	√	√	√	√
Security Awareness	√	√	√	√	√	√
Risk Assessment	√	√	√	√	√	√
IT Security Assessment	√	√	√	√	√	√
Security Policies and Procedures	√	√	√	√	√	√
Database Auditing & Protection		√	√	√	√	
File Activity Monitoring & Protection		√	√			
Data Loss Prevention		√	√	√	√	
Data Masking			√	√		
Web Application Firewall				√		
Email Security & Encryption				√		
Secure File Synchronization & Sharing				√		
Hard Drive Degausser						√
Data Wiping						√
Security Information & Event Management		√	√	√	√	

"GDPR: Get it right now or take the risk"

ODYSSEY
Impossible Challenges, Possible Solutions

HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades str. 2012
Strovolos, Nicosia

Tel.: +357 22463600
Fax: +357 22463563

Email: info@odysseycs.com

OFFICES:

CYPRUS | GREECE | SERBIA | UAE | USA | SOUTH AFRICA