

General Data Protection Regulation

GDPR: General Data Protection Regulation

CubelQ Approach on GDPR Compliance

EU Regulation 2016/679 of the European Parliament and the of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation.

Following four years of preparation and discussion, the General Data Protection Regulation -GDPR was finally adopted by the EU Parliament on **14 April 2016** under regulation number **2016/679**.

It has entered into force 20 days after its publication in the Official Journal of the EU and will be directly applicable in all Member States two years after that date, i.e. **25 May 2018**, so that organizations that do not comply will face heavy fines.

The General Data Protection Regulation replaces the EU Data Protection Directive 95/46/EC and aims to:

- (a) Harmonize data protection laws across Europe;
- (b) Protect and strengthen the protection of privacy of EU citizens and
- (c) Reform the way in which organizations operating within the EU, approach and manage privacy issues.

When GDPR is Applied:

- The date in which GDPR will be in force in EU Member States is **May 25, 2018**

How GDPR is Applies

- After **May 25, 2018** companies operating within the EU should use high-tech security systems to protect the personal data they manage.

Penalties in Case of Infringement

- In the event of a personal data breach, businesses must (a) inform the local - national private data protection authority and their local - national regulatory authority and (b) communicate directly will individuals whom data breach affected or do a public announcements
- Organization with GDPR breach will be fined up to 4% of their annual turnover or EUR 20 million (whichever is greater)!

General Data Protection Regulation

Businesses Obligation

A. Follow the basic data protection principles, namely:

- Collect personal data for a specific legitimate purpose and collect only those of them which are necessarily for achieving the specific purpose.
- Do not process them further in any way incompatible with that specific purpose.
- Update them on a regular basis.
- Store them for the minimum time period required.
- Obtain per case the free and clear consent of individuals for whom personal data are collected.

B. Transfer personal data to non-EU countries only under certain conditions.

C. Give access to personal data managed to partners only under controlled and secure conditions and only if they demonstrate their compliance with GDPR.

D. Develop and use electronic computerized procedures and tools for timely and free or charge requests of individuals to:

- Recall of their consent.
- Have access to their personal data.
- Correct their personal data.
- Delete their personal data.
- Reduce of processing their personal data.
- Receive their personal data in electronic form.
- Transfer their personal data to another legal entity.

E. Notify and inform the individuals appropriately and promptly about their rights on personal data protection and management.

F. Ensure personal data protection throughout their life cycle.

G. Keep records and inform for any personal data breach within 72 hours the National Private Data Protection Authority and the individuals with direct communication and public announcements.

H. Be able to prove that you comply with all GDPR requirements.

CubelQ Approach to GDPR Compliance

In CubelQ we have the tools, methods and procedures to make any business that maintain and manage personal data compliant with the General Data Protection Regulation **2016/679/EU**.

Data Security & Identity Management

Encryption Systems, Hardware Security Modules – HSM

- General Purpose HSMs
- Transaction & Payment HSMs
- Customizable HSMs
- Network HSMs, USB HSMS, PCI Cards

Unstructured data, structured data, database, disks and files protection & encryption:

- SafeNet ProtectApp: Encrypt sensitive field and application data at the point of creation
- SafeNet ProtectDB: Protect sensitive data across databases in the data center and the cloud

General Data Protection Regulation

- SafeNet Tokenization: Tokenize sensitive data entering your organization and achieve compliance
- SafeNet ProtectFile: Encrypt the data in and control access to sensitive folders and files
- SafeNet ProtectV: Securely increase data center virtualization and/or migrate to the cloud
- SafeNet KeySecure: Manage cryptographic keys, certificates and applications with a single, centralized platform

Network and WAN protection & encryption - Ethernet Encryptions

- CN6000 Series: up to up to 10Gbps
- CM8000 Series: Layer 2 network Ethernet and Fiber Optic, up to 100Gbps
- CN4000 Series: entry-level from 10Mbps to 1Gbps

Public Key Infrastructure - PKI

- Full PKI environment deployment
- PKI Key(s) Management, PKI Encryption & Decryption of Data
- Signatures and Certificates Generation & Authentication

Digital rights management – DRM

- Digital Rights Management for document distribution
- Adobe PDF, Microsoft Word, Excel & P

Multi - factor authentication

- Full PKI certificate life cycle management
- Physical OTP (time & event) tokens
- Soft OTP, TAN Matrix, passwords,
- Out of Band – OOB OTP
- Mobile OTP
- Bluetooth PKI and/or OTP
- Pattern based OTP

Physical & Logical access control

- Physical access control with Centralized Management
- Same medium Physical & Logical access control with Centralized Management

End point security

- Clientless End point security for Monitoring and Enforcing Security Policy

For more information please contact:



CubelQ Ltd.

78 Vyzantiou St., 14234, Athens, Greece.

Tel: (+30)-210-9530242

Fax: (+30)-210-6255672

Email: info@cubelq.gr

Web: www.cubelq.gr