

# Are You Ready for GDPR?

## Authentication and Access Management Solutions for GDPR Compliance

### 1. What is GDPR?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was created to strengthen the safeguards around personal data and create a more uniform standard within the European Union (EU). Created by the European Parliament, the Council of the European Union and the European Commission, GDPR replaces the 20-year-old Data Protection Directive (the "Directive") as the EU's primary data protection law.

***GDPR mandates the procedures and dictates the consequences regarding data breaches and notification.***

### 2. Who is affected by GDPR?

Any organization that handles personal data of EU citizens, whether that organization is located in the EU or elsewhere.

### 3. When did it take effect?

GDPR went into effect in May 2018.



Maximum Fine 4% Global Turnover or €20,000,000 (whichever is higher).



Deadline to tell Authorities: 72 Hours.

Deadline to tell users: "without undue delay."

### 4. Big penalties for non-compliance.

If there is a Data Breach:

### 5. How Authentication and Access Management Help Comply with GDPR.

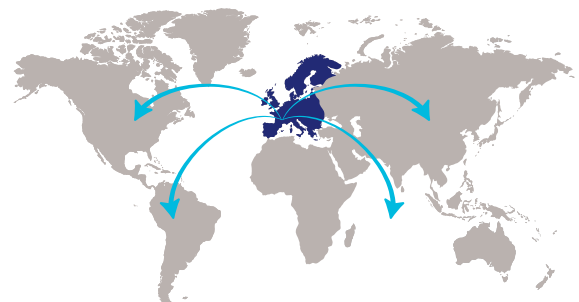
#### Authorized Access

Organizations will need to verify the legitimacy of user identities and transactions, and to prove compliance.

#### Digital Signature and eMail Encryption

GDPR requires organization to prove the existence of appropriate safeguards when processing data outside of its originally consented use. Advanced authentication and access security features, such as digital signature and email encryption, help ensure secure dissemination of private data.

Thales offers the only complete portfolio of Authentication and Access Management solutions, including cloud access management, PKI, certificate-based authentication, one-time password authentication, identity federation, complete lifecycle management and auditing tools.



#### GDPR is essentially the first global data protection law.

The regulation also applies to non-EU companies that process personal data of individuals in the EU.

The international transfer of data will continue to be governed under EU GDPR rules.



**All companies globally can be fined.**

## 6. Thales Access Management and Authentication solutions for GDPR.

**SafeNet Trusted Access (STA)**—is an intuitive cloud access management service that makes it easy to manage cloud access with cloud single sign-on and scenario-based access policies. By combining the convenience of single sign-on with granular access policies, organizations can tighten access controls, and reduce password fatigue.

**Certificate-Based Authentication (PKI)**—Thales' comprehensive public key infrastructure (PKI) authentication solutions provide military-grade security. Supporting a wide portfolio of SafeNet IDPrime smart cards and SafeNet USB eTokens, Thales' authentication management solutions ensure the proper security controls are in place to verify the identity of users and enable advanced security applications such as authentication, digital signing and encrypted email on any PC, desktop or mobile device.

## Mapping Thales Authentication Solutions to GDPR

### *Article 5: Principles relating to processing of personal data*

**Summary:** However data is processed, it needs to be secured from unauthorized access and loss.

**Solution:** As a first line of defense, Thales authentication solutions ensure only authorized users have access to processing systems. Asking for a second authentication factor ensures that a simple stolen password won't be sufficient to gain unfettered access to sensitive systems.

### *Article 24: Responsibility of the controller*

**Summary:** Organizations are required to take reasonable security measures that respond to the likely risks and threats they face.

**Solution:** Thinking beyond the data itself, organizations can use Thales authentication solutions to restrict access to corporate networks, protect the identities of users, and ensure users are who they claim to be. As a first line approach to data security, requiring multiple factors of authentication to verify a user's identity helps mitigate the risk of unauthorized users accessing sensitive systems to manipulate data.

### *Article 32: Security of processing*

**Summary:** Organizations will need to consider the risk associated with data processing such as data loss and unauthorized access when choosing the right level of security.

**Solution:** Thales' authentication solutions make it harder for unauthorized users to access sensitive environments while also mitigating risk posed by administrators with privileged access. Thales authentication offers a complete set of provisioning rules and policy engines that cover privileged users and the varying levels of security they may need for their roles. Organizations can increase or decrease the level of access security to their data and network according to the level of sensitivity of the data concerned.

### *Article 33: Notification of a personal data breach to the supervisory authority*

**Summary:** Organizations will need to ensure individuals only process data when authorized

**Solution:** Thales authentication solutions automatically apply rules in real time to users based on their group membership and their need to access certain levels of private data. The rules' default setting can keep users out of processing systems, or offer only a narrow level of access, until instructions are given from the data controller. Once processing is complete, administrators can return settings to a more restrictive default that prevents any further data processing. In addition, all of Thales' SafeNet authentication solutions provide extensive log and report mechanisms to give up-to-date snapshots of all authentication and management events.

Thales' portfolio of SafeNet authentication solutions gives organizations navigating GDPR the tools they need to solve these challenges according to the shape of their operations and their IT architecture.