CERTES NETWORKS

General Data Protection Regulation (GDPR) in the United States

Why you should care and what you need to know!

eBOOK |

The GDPR has legal effect in the United States – True or False?

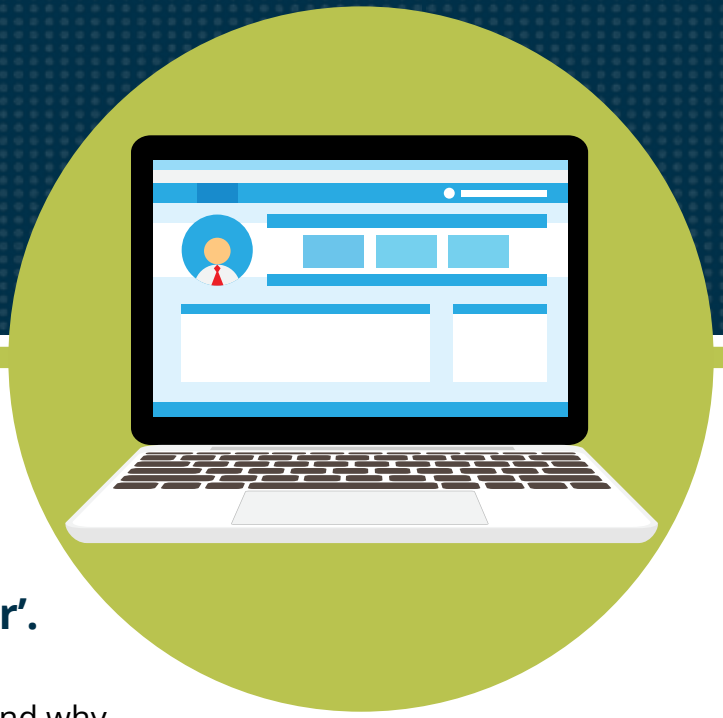
FACT | The GDPR applies to organizations established outside the European Union if such organization:

1. Processes the personal data of EU residents when offering them goods or services (Article 3(2a)) or;

2. Monitors the behavior of EU residents (Article 3(2b). "Monitoring" may include tracking an EU resident on the internet and may also include the use of data processing techniques to profile individuals, their behaviors or their attitudes in order to analyze or predict personal preference.

If you have customers in Europe and either of the above criteria applies to your organization then you must comply with the GDPR.

How do I comply?



Your obligations under the GDPR will vary according to whether your organization is considered to be a data 'Controller' or 'Processor'.

A 'Controller' is the entity that determines the purpose for which, and why, personal data is processed. A 'Processor' is any entity that processes personal data on behalf of the data controller. For example, a bank collects certain data from its clients when they open an account (so is deemed to be a 'Controller') whereas a third party technology provider will often store and host that data, and will therefore be a 'Processor'. Controllers are subject to more onerous obligations than processors. It is important to first identify which category your organization is considered to be.

What else do I need to know?

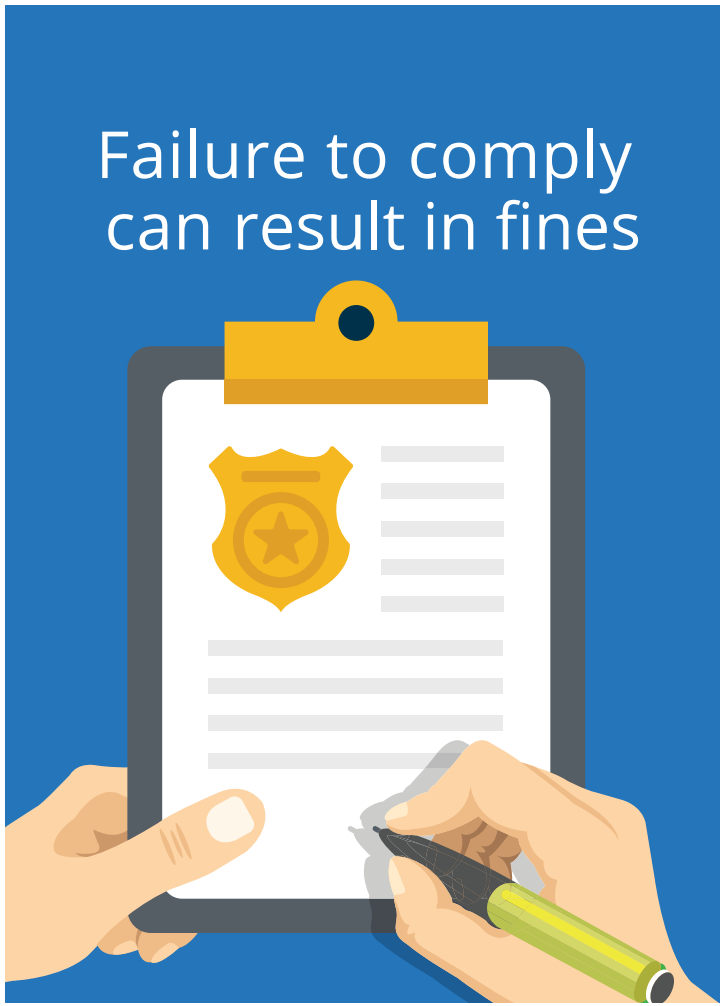
The GDPR is complex with numerous obligations. However, some of the key challenges that you should be aware of are:

Lawful, Fair, and Transparent Processing

There are several requirements that need to be met to ensure that personal data is processed lawfully and fairly. For example, except for under a limited set of circumstances, an individual's consent will be required that their personal data can be processed for a specific purpose. Such consent must be freely given and unambiguous (silence and pre-ticked boxes do not constitute consent). Entities are also obliged to tell individuals what their personal data is being used for. Personal data must be accurate, relevant and limited to what is necessary in relation to the purpose for which it is being processed. Entities cannot collect data and then decide the purpose for using it at a later date – the purpose must be designed from the outset.

Rights of Individuals

Data subjects have various rights. They can request from controllers access to the personal data that is being stored. They have the right to request that any inaccurate personal information is rectified, and the right to prevent processing taking place in certain circumstances.



Data Security

Both controllers and processors must ensure that personal data is kept secure from both external threats (e.g. hacking) and internal threats (e.g. poorly trained employees). Article 32 specifically requires that entities: "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data". Therefore, the use of encryption can help mitigate the risk of reputational damage.

Fines

Penalties can be administered for non-compliance. The maximum fine a controller faces for non-compliance with the provisions of the GDPR is 20,000,000 EUR or up to 4% of an organization's annual worldwide turnover. In the case of a processor, the maximum fine is 10,000,000 EUR or 2% of an organization's annual worldwide turnover.

Name and Shame

Another major concern is that in the event of a personal data breach, a controller must report such breach to the relevant supervisory authority within 72 hours (where feasible). Clearly this timescale is very challenging and so organizations should consider their internal reporting and escalation processes are sufficient to achieve this.

Furthermore, if a data breach poses a high risk to individuals, (for example, hackers gain access to an individual's credit card details), then the entity has to notify those individuals. This can result in severe reputational damage. However, there is a 'Get-out-of-Jail' card. Article 34 (2) provides that an organization can avoid having to make this disclosure: "if the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption".

Representatives

Companies that do not have an office in the EU yet provide their products or services there must appoint a representative in the EU if they process personal data. The EU-based representative serves as the first point of contact with the organization and both data subjects and the data protection supervisory authorities. This helps to ensure that the GDPR is adhered to and enforced.

Are there specific activities/ industries that are more at risk?

Certain industries, by the very nature of their business, could be more at risk.

For example, organizations that process data on large scales (e.g. banks, social media networks) face a higher degree of risk due to the large number of individuals affected by database errors or breaches. Organizations that carry out profiling activities (e.g. tracking customers' browsing habits to offer relevant products, or automated refusal of credit card applications) conduct activities that affect the privacy of individuals and face a higher risk.

When is the deadline and what do I do next?

The GDPR takes effect May 25th, 2018. A complex program of work will need to be undertaken in order to be ready, and so a crucial first step is to ensure that your organization has the right roles in place to deliver that program. One key role is the appointment of a Data Protection Officer who will take responsibility for implementing it.The program should ensure that the organization can demonstrate accountability for all processing activities transparently and that data flows into the EU are understood. It should also ensure that the right processes are in place to ensure data subjects can exercise their individual rights. Different expertise will be needed to ensure that the compliance program is fit-for-purpose, including lawyers, document management experts, IT specialists, security experts and external consultants.

For further information on GDPR Compliance or to find out about any upcoming GDPR information sessions from Certes go to CertesNetworks.com or email info@certesnetworks.com.

How Can Certes Networks Help?

The below sets out how Certes Networks' solution can help achieve compliance in key areas.

GDPR REQUIREMENT	RESOLUTION	HOW CERTES NETWORKS HELPS
Security of Personal Data Article 32	Both controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including: a. the pseudonimisation pseudonymization and encryption of personal data b. the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services.	• Certes Next Gen Encryptors are multi-layer encryption devices offering Layer 2, Layer 3 or Layer 4 encryption. They can provide protection for any network. • Integrating easily into any existing network, Certes Networks' overlay solution requires no re-architecting of the network, enabling encryption to be rapidly deployed. • Operating transparently within the network infrastructure, there is no performance degradation; ensuring essential transactional systems operate without impact.
Communication of a Personal Data breach to the Data subject Article 34	Communication in the event of a breach may not be required if the controller has implemented appropriate technical and organization protection measures – such as encryption.	• Even if an encrypted network is breached, companies may be free from the notification requirements of GDPR to data subjects since all data is subject to a powerful combination of encryption and authentication. • Organizations can avoid the reputational damage associated with high profile breach.
Principles relating to processing of personal data Article 5	Appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. (Integrity and confidentiality)	• Certes Networks' encryption delivers confidentiality. • To maintain confidentiality and integrity, Certes Networks encrypts and authenticates every packet. • Packet authentication guarantees every packet received is identical to the packet sent, thus preventing interception, modification or replay attacks.

About Certes Networks

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you “Encryption without Compromise”.

For more information visit **CertesNetworks.com**

Global Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
Tel: +1(888) 833-1142
Fax: +1(412)262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East & Africa Sales
emea@certesnetworks.com

V1-10-19-2017