CERTES
CERTESNETWORKS.COM

WHITE PAPER |

CERTES NETWORKS – COMPLIANCE SOLUTIONS

General Data Protection Regulation

The primary objectives of the General Data Protection Regulation (GDPR) are to give citizens and residents back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European Union (EU).

Starting in May 2018, GDPR will replace the Data Protection Directive from 1995.

GDPR Requirements

Given the current regulatory environment – not least the long standing Data Protection Directive - many of the demands of GDPR will have already been met. From appointing a CISO to adopting a written cybersecurity policy, good security practices will address a large part of the GDPR requirements. However, there are a number of new requirements which firms need to be aware of, including;

- Pseudonimisation of personal data
- The importance of confidentiality (encryption) for protecting personal data
- Integrity and availability in all data processing
- Obligation to report a data breach to the applicable supervisory authority within 72 hours
- Data subjects may need to be notified of any breach. This will result in severe reputational damage to the company
- Potential fines for non-compliance are significantly higher compared to those under any previous data protection laws (Up to €20 million or 4% of an organization's global annual revenue, whichever is greater)

How does Certes Networks help you comply with GDPR?

Certes Networks' network encryption solutions are quick to deploy and easy to manage. They rapidly deliver the confidentiality, integrity and availability (CIA) required by GDPR. The Certes' Next Gen Encryptors provide multi-layered data protection and application segmentation. Certes' Encryptors integrate easily into any existing network. They operate transparently to the network infrastructure. They ensure all data is encrypted without impacting overall network performance.

- **Safeguard Reputation:** When a breach occurs, organizations that use encryption as a security measure may be exempt from the legal requirements for notification to the data subjects. This minimizes the risk of damage to the reputation of the enterprise. This also lowers public awareness of the data incident.
- **Confidentiality:** Packet level encryption protects data in motion across any network.
- **Integrity:** Per packet authentication prevents the injection of rogue packets into your network.
- **Ease of Deployment:** 100% Software-Defined security overlay eliminates the need to re-architect the network or replace legacy applications.
- **Scale:** Supports your national or global infrastructure across multiple provider networks.

Copyright © 2017 Certes Networks, Inc. - All Rights Reserved. | CERTESNETWORKS.COM

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.

CERTESNETWORKS.COM | Copyright © 2017 Certes Networks, Inc. - All Rights Reserved.

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

V1-06-01-2017