ZYXEL

ditor code={code} onChange={onChange} />
button type="button" className={classes.hideCode}
Hide code
</button>
iv>
utton type="button" className={classes.showCode}
Show code
/button>

What does GDPR mean to SMBs

Trust Zyxel. Your Networking Ally

The Clock is Ticking...

2017 has been a challenging year in security! Ransomware, the cryptoworm WannaCry and their effects have regularly been in the press. In 2018 the security situation has not relaxed. On the contrary - 2018 will be even more demanding. With this in mind, it is critical to ensure that your business is adequately protected. This has never been more important with the clock ticking down to GDPR. On 25th May 2018, the new General Data Protection Regulation will come into force, better known by the acronym "GDPR".

Many small businesses mistakenly think that this regulation doesn't apply to them or will not affect the way they operate; whilst others are ignoring it and hoping it will go away.

The regulation replaces the existing data protection laws of individual countries, clarifying and consolidating these laws into one. With these changes comes the added requirement for more stringent security.

There is an overwhelming amount of information readily available for businesses to access on the data collection and processing side of compliance, how to ensure opt-in and preserve the right to be forgotten. However, your security strategy should be a vital part of your plan that isn't over looked - data breach prevention planning is now essential. How do you identify where your security is deficient and liable to a breach and how do you fill the gap with an effective solution?

GDPR Overview

The new GDPR replaces the Data Protection Directive 95/46/ec and lays out a minimum set of standards for protection of EU Citizen's personal data and the free movement of data within the EU. In the new regulation, the concept of privacy and data protection redefines "personal data" to extend this to online identifiers such as IP address, cookies and geolocation data. Genetic, mental, health, cultural, economic and social information will be classed as sensitive personal data, which needs to be anonymised and encrypted.

Companies must ensure that compliance is in place before the effective date of 25th May 2018. The regulations will apply to each member of the EU, Brexit-UK and extends the jurisdiction to all companies that process personal data of persons residing in the European Union regardless of the geographical location of the business or the place where the data is handled or processed.

Overlooking or not putting adequate processes in place for GDPR can have costly implications. Companies that do not comply risk fines of up to €20 million or a fine up to 4% of the total annual turnover whichever is highest. Individuals have the right to seek compensation for both minor and major breaches of the regulation.

Data Collection and Processing under GDPR

For data collection and processing under GDPR, companies must demonstrate:

- ✓ An explicit consent has been received from an individual for all personal data collected about them - clear opt-in.
- ✓ That the reason for data collection is clearly specified, explicit and legitimate in purpose.
- ✓ Personal data is processed - profiled and segmented lawfully, fairly and in a transparent manner.
- ✓ Processing should not take place for reasons outside the initial purpose specified.
- ✓ Data held should be accurate and up-to-date.
- ✓ Data should only be kept for as long as necessary.
- ✓ That if an individual exercises their right to be forgotten, have visibility of the data stored about them or have any stored data updated that there is a clear process.
- ✓ Any requests to update data, be forgotten or disclosure of what is held is handled within 1-month of the request.

Zyxel Unified Gateway Series integrated security defense technology

The Challenge - securing your data to minimize your risk

Historically, companies have chosen to minimize the implications of a breach, failed to be transparent, or in many cases not even known the extent of a breach. With GDPR there is no hiding place. Data breaches must be reported immediately to data protection authorities and affected individuals; ideally within 24-hours, but certainly within 72-hours. Even a small breach could be enough to shut your business down whether it is from the cost of the fines or lost reputation.

Appropriate protection from accidental or unlawful destruction, loss or alteration of personal data is required. Adequate security and monitoring is not an option but a business essential tool to ensure no- unauthorised access or disclosure of any data held. To achieve compliance businesses must put into place governance measures that include detailed documentation, registration and evaluation of security risks.

To stay compliant business need to employ encryption and powerful real-time data protection measures that use innovate and constantly updated network security technologies.

Zyxel security "by design"

Zyxel's Unified Security Gateway (USG) series offers highly integrated defence technology to provide the best protection for small and medium businesses covering all of your GDPR compliance needs. You can rest assured that you have unbeatable protection from malware and unauthorized applications via IDP inspection. Your data encryption requirements are met through IPSec and SSL VPN tunnel technology. Security "by design" means Zyxel can offer customers a comprehensive, powerful and scalable solution that adapts to your GDPR requirements. Through licensing, you have the freedom to select and design the functionality that fits with your business or opt for the full compliment.

Anti-Virus

Prevents the latest content layer threats by detecting and removing malware.

Firewall

Monitors and controls the incoming and outgoing network traffic

Anti-Spam

Reduce the number of spam messages, control attacks and virus infections via email

Application Intelligence

Allows or denies the use of web applications to prevent threats from entering the network through applications

Intrusion Detection & Prevention

Checking against network traffic flow to prevent known and unknown stealth cyber threats

WLAN Controller

Integrated in a WLAN control gateway to the radio receiver, reducing the cost of multi-machine deployment

Content Filtering

Prevents inappropriate content and dangerous sites on the Internet by blocking connections

VPN

Support a variety of high-end encryption technology to ensure that mobile users and network communication between the network

Next steps to take action against ransomware

Understand your security requirements with our security audit

Contact Zyxel for a free consultation

For more product information, visit us on the web at www.zyxel.com Copyright © 2017 Zyxel Communications Corp. All rights reserved. Zyxel, Zyxel logo are registered trademarks of Zyxel Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.