GDPR

GETTING READY FOR GDPR

Cybersecurity for Data Protection

The General Data Protection Regulation (GDPR) is the European Union's response to the increasing privacy demands of the European society. The primary objective of the GDPR is to establish personal data as property and to shift control of said property to the individual or user, rather than to the business or provider.

Furthermore, the GDPR will come into force shortly and many companies are simply not ready to comply with the more stringent standards of using, moving and storing customer data. Let's analyze the full scope of GDPR and what it means for your cloud strategy.

GDPR

Overview

Protecting personal data has been an important issue in the European Union (EU) for more than 20 years and the recently ratified GDPR takes data protection to an entirely new level. In addition to a new set of legal requirements that necessitate both organisational and technological responses, the GDPR is also applicable to organisations around the world that collect or process data on residents living within the EU, including permanent residents, visitors and expatriates.

Per the standards set forth in the GDPR, regulatory compliance will now be predicated on the geographical location of the individuals whose personal data has been collected –not the location of registration for the organisation that collected the data. Therefore, meeting the intent of GDPR will require serious attention and action from all organisations doing business across Europe (including the United Kingdom post-Brexit), both in the EU and in the European Economic Area (EEA).

The GDPR also gives EU residents the right to request their personal data from organisations who collect and house such data and also to withdraw consent of its use, thus effectively ordering the destruction of personal data. Article 12 of the GDPR, which covers the rights of the data subjects and the transparency associated with the handling of such data, specifies that any such request for access or destruction of personal data must be free of charge, easy to make and must be fulfilled without 'undue delay and at the latest within one month.' However, since most organisations will require significant time and investment to support GDPR-mandated processes and capabilities, the EU has extended the implementation date until May 2018 for required compliance. But given the GDPR's sweeping scope and transformative impact, it is imperative that organisations review – and most likely overhaul – the way they handle personal data today.

GDPR Key Points

An overview of the main changes under GDPR and how they differ from the previous directive. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different than when the previous directive was established in 1995. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR, as well as information on the impacts it will have on business can be found below:

Increased Territorial Scope

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the geographical area known as the EU, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in several high-profile court cases. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether

the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also be required to have a representative in the EU.

Penalties
Under the GDPR, organisations found in breach can be fined up to **4% of annual global turnover or €20 Million** (whichever is greater), which is currently the maximum fine that can be imposed for the most serious infringements (e.g. Not having sufficient customer consent to process data or violating the core of Privacy by Design concepts). However, fines will be levied using a tiered approach, depending upon the scope of the violation (e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment). It is important to note that these rules apply to both controllers and processors – meaning cloud-service providers will not be exempt from GDPR enforcement.

Consent
The GDPR also intends to require the simplification of terms and conditions, since modern Ts&Cs have become virtual landfills of expansive legalese filled with illegible rubbish aimed at protecting the originator rather than informing the actual customer. The new regulation will require Ts&Cs, along with consent requests for the purposes of data processing to be intelligible and in easily accessible form, using clear and plain language. Furthermore, the ability to withdraw consent must also be easily obtainable.

Privacy Restored
Whether your business stores data in-house or in the cloud, the bottom line is that the privacy and security of collected data must be maintained.

Smart businesses should already be adhering to many of the principles set forth in the GDPR with the goal of minimizing any risks associated with privacy in today's world. It's also wise to review all the data your company currently stores from your customers to ensure that you are only collecting the data you need and the data that you said you would be collecting. Companies – especially those outside Europe where businesses store customer data for marketing purposes – will need to consider an overhaul of databases and any associated client data.

When developing and using applications, services and products that process personal data, a strict review process for data collection and protection should always be in place. Taking a proactive approach to data collection from the perspective of the user may also help you to comply with any future requests from clients who may wish to have their privacy restored by deleting such data.

Getting ready for 2018

Realistically, most regulations are far from precise when trying to set compliance standards and establish baseline requirements

GDPR

from organisations and their IT departments. As with most associated privacy regulations, the GDPR does require applicable organisations to apply best practices and to have certain protection processes in place to better protect the privacy rights and data security of their customers. However, it doesn't specify particular security solutions that should be deployed, for example, which can present certain challenges for IT departments. Yet the GDPR still requires a complete approach to information security, demanding best practices, adequate documentation and effective types of protection.

With that in mind, here are just a few best practices organisations should be thinking about now to prepare for GDPR when the new regulation comes into play in **May 2018:**

- Conduct a data audit to find out what data you hold and how you are using it
- Classify data per sensitivity and disregard any non-critical or needed customer data, therefore minimizing risks
- Email archiving and data backup should be monitored and rules applied to avoid unintentional (and intentional) incidents
- Staff awareness and user education training programs to focus on data protection
- Ongoing review to determine and define exactly which users should have limited access to client's data
- Consider using two-factor authentication for any account with sensitive data access
- Implement a multi-layered security approach for both email and corporate networks to prevent phishing and ransomware attacks
- Develop a data breach response plan to ensure you can report within 72 hours
- Designate a Data Protection Officer (DPO) if you are an enterprise – in line with the GDPR requirements

How can AppRiver help?

At its core, privacy by design calls for the inclusion of data protection from the onset of a system's development, rather than a later addition. More specifically in line with GDPR intent – 'The controller shall…implement appropriate technical and organisational measures…in an effective way…in order to meet the requirements of this Regulation and protect the rights of data subjects'. AppRiver's set of Advanced Threat Protection solutions and Email Encryption capability enables SMBs to protect against security and data breaches with an enterprise-grade multi-layered approach to security.

GDPR

Security and Privacy by Design
Security and privacy by design are integral to securing your customer's data. As part of a legal requirement thorough the GDPR, it becomes critical to have a throughout plan in place. Documenting each layer of defense and your privacy policy will allow your organisation to provide potential and existing customers assurance that the provided protection can help them meet the intent of the regulation.

Audit and Monitor your Network
Every business, including yours, has valuable IT assets such as computers, networks and data. Protecting those assets requires that companies of all sizes conduct IT security audits to get a clear picture of the status of their network, the security holes they face and how to best deal with those threats.

If you already have Web Protection deployed on your network, it is advised to run a network audit using the monitor options available and to deploy the network usage and threat analysis. This will produce a report providing you with critical information on the health of the network and list any malware found. If any malware is detected, Web Protection will automatically block the attempt and give your administrators time to clean up the infected PC. Also, be sure to create a master list of the assets your company has so you will be able to decide which assets require protection. That list of assets should include PCs, mobile devices, laptops, routers, VoIP phones, IP PBXs, networking equipment and printers at a minimum.

Multi-layer Security
Securing a network with a multi-layer approach is a best practice. Your organisation should protect all security holes by combining Email and Web Security solutions with an Endpoint AV protection layer. AppRiver's Web Protection platform and Advanced Email Security solution will complement AV endpoints by blocking malware at the source, as well as scanning networks in search of resident malware that went untraced in the past and could potentially be calling home under the right circumstances. By deploying the right combination of Email Security, Network & Web Security and Endpoint AV, your business can close the security gaps available in each network and gain inbound and outbound traffic monitoring.

Email Encryption
Email can travel a long way before it hits your inbox. With Email Encryption from AppRiver, you'll avoid prying eyes along the way. With one click, Email Encryption encrypts your message when it leaves your mailbox. Only the authorized recipient – with the proper password – can read the message, which keeps the client's data private and protected along the way. AppRiver's email encryption gives you true mailbox-to-mailbox security, no matter where your email goes in between, ensuring that data privacy is maintained.

Email Encryption will help you to fulfill the 'accountability' demanded in article 5:2 of GDPR. Use the delivery slip option to audit and verify the status of all your encrypted emails at any time.

Related solutions

Email Security
Web & Network Protection
Email Encryption

appriver.com
sales@appriver.com
(866) 223-4645