The EU General Data Protection Regulation

Understanding the Data Protection requirements and how to comply.

A lot has changed since 1995, the last time a major European law was passed on the subject of data protection (the Data Protection Directive 95/46/EC). For example, mobile devices are ubiquitous, and it’s not unusual to carry two or even three at a time. Meanwhile, sensitive company data is moving outside the safety of the traditional corporate security perimeter. Employees email documents to themselves, access data from personal smartphones and tablets, and store data in the cloud. Major personal data breaches are commonplace today, putting customers at risk of identity theft and financial loss, and businesses at risk of losing customer and investor loyalty, as well as regulatory fines. This whitepaper discusses what the General Data Protection Regulation (GDPR) will mean to organizations globally.
Why are the changes needed?
Like the majority of states in the U.S., all countries in the European Union (EU) have implemented data protection laws to reflect this new reality of the dissolving network perimeter. As with the differences between U.S. states, the European data protection regulations currently vary from country to country. There has not been a significant overhaul of EU data protection regulations in some time. This, paired with the need to address the major technological developments since 1995, has driven efforts to modernize and homogenize the EU Data Protection regulations.

The GDPR is the culmination of years of work by the EU to reform Data Protection regulation into a Union-wide framework instead of a patchwork of country-specific legislations (the GDPR does permit certain county-specific derogations to be made, such as the age of consent for submitting personal data). The GDPR takes the form of a regulation, meaning that it applies directly in every member state in the form in which it was passed. Previous data protection legislation in member states stemmed from a directive which each country implemented into its national legal system with a degree of flexibility, leading to differences from country to country. The regulation is intended to strengthen the privacy rights of EU citizens, restore confidence in online activities and better protect customer data by requiring companies to adopt new data protection processes and controls.

The regulation officially entered into force on May 24, 2016, and from this point countries had up to two years to implement the new requirements. However this was the upper limit to implement the changes and countries such as the Netherlands chose to update its data protection laws sooner.

The text itself consists of 99 articles and like any piece of legislation can be confusing. Our goal with this whitepaper is not to educate readers on the entirety of the law, but instead to focus on the need to protect the security of personal data, which falls under the most severe set of proposed fines. To learn more about the regulation, please visit the resources listed in the appendix of this document.
Core Elements of Reform

In this section we have extracted some of the key articles related to keeping personal data secure and the potential consequences of failing to do so.

**Article 32** addresses the security of processing data:

1. **Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:**
   
   (a) The pseudonymisation and encryption of personal data;
   (b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services processing personal data;
   (c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Put simply, the article requires organizations to implement appropriate security measures to protect personal data. The article makes specific reference to ‘encryption of personal data’ as one of the means to achieve this.

The article also mentions the ‘ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services processing personal data’. In regard to encryption technology, this means having a robust key management procedure in addition to encrypting your data. The wider implications are having a sound disaster recovery plan in place.

Should a personal data breach occur, **Article 33** specifies that the company is required to notify the supervisory authority within 72 hours after having become aware of the breach. However, the company may or may not be required to notify individuals whose data was breached. **Article 34** states:

1. **When the personal data breach is likely to result in a high risk of the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.**
2. (...)
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption;
(b) The controller has taken subsequent measures which ensure that the high risk of the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or
(c) It would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If, at the time of the loss, the personal data was protected in such a way as to be unintelligible (and therefore useless to an unauthorized party, such as via encryption) – and the company can prove this to the supervisory authority, then the company is not required to disclose the breach to the individuals whose personal data was lost or stolen.

If a company fails to do any of these things – adopt internal policies and implement appropriate measures for ensuring and demonstrating compliance, or notify the supervisory authority or the data subject of a personal data breach, where appropriate – then Article 83 on Administrative fines sets out the potential maximum sanction as:

1. Infringements of the following provisions shall, in accordance with paragraph 2a, be subject to administrative fines up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

To summarize: If you don’t put the right technology in place to protect personal data, then you may have to pay – directly to the supervisory authority and indirectly from reputation damage, and loss of goodwill and customer trust. However, companies that encrypt their data, protect their customers – and themselves.
GDPR: Understanding the Data Protection Requirements and How to Comply

Regulation enforcement

The GDPR greatly strengthens enforcement powers. The new maximum fines of €20 million or 4% of annual worldwide turnover are a significant increase on what could previously be enforced. For example in the UK, the Information Commissioner’s Office could only implement up to a £500,000 fine. Which means the consequences of a breach have become much more significant.

Who is impacted by the GDPR?

The GDPR should be of global interest, as it impacts any company doing business with European citizens – regardless of where the company is based. This is very similar to many US data protection laws. For example, a company based in France doing business with American customers in California must comply with California’s data protection law. If that same company also does business with customers in Massachusetts, then it must also comply with Massachusetts’ data protection law, and so on. Some of the benefits of the new legislation are:

- One EU market, one law – European and non-European companies no longer need to research and know the details of 28 different rules and regulations.
- Unified process – The same process will be followed in case of breaches and/or violations.
- Same rules apply to all companies – Regardless of where the companies are based, the same rule set will apply when doing business within the EU.

How to Comply with the GDPR

For the many companies that must comply with the new legislation, the best way to prepare is to implement a solid data protection strategy that guards against loss of data whether through malicious or accidental methods.

While the new legislation does not require a specific type of technical control, it does make several references to encryption as a means to secure personal data and render it unintelligible to unauthorized users. So how are organizations achieving compliance with other regulations that seek to protect personal data? The Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and Sarbanes-Oxley (SOX) are a few examples of regulations that require data protection controls similar to those in the EU Data Protection Regulation. Because it renders data unintelligible, encryption is widely accepted as an adequate means of addressing these requirements. If encrypted data becomes lost or stolen, it is essentially worthless. No one can access the actual data. And when encrypted data is combined with security systems that stop data-stealing attacks you have the best chance of keeping your data safe.

**Bottom line:** If you want to ready for the Data Protection Regulation changes, you should look at encryption and anti-malware technologies.
How Sophos helps you meet the data protection challenge

Creating a data protection strategy can be a daunting process, especially if it hasn't previously been a focus area for your organization. So where should you start? A solid data protection strategy isn't built in a day. But consider that 58% of data breaches are due to hackers or malware and 27% of data breaches are caused by unintended disclosure (human error). Securing against these threats is a great place to begin and Sophos recommends three steps to achieve it.

**Stop hacking and malware**

Malicious attacks that employ data-stealing malware are a major cause of data breaches. Sophos XG Firewall stops threats at the door before they can penetrate your network, and stops from spreading inside the network.

Sophos Intercept X and Central Endpoint Advanced keep your endpoint devices safe from data-stealing attacks with anti-malware, anti-exploit and anti-ransomware protection.

Sophos Server Protection secures your servers against advanced malware threats including ransomware. Keeping your organization’s most sensitive data protected.

**Secure devices even if lost or stolen**

Misplacing a device or theft of a device is no defense against the GDPR. Sophos Central Device Encryption is the easiest way to centrally manage full disk encryption for all of your PC's and Macs, keeping your data secure even if it is lost or stolen.

Sophos Mobile utilizes secure containers to keep sensitive data isolated and secure. In the event a device is lost or stolen it can be remotely locked and wiped.

**Reduce impact of human error**

Most of us have sent an email to the wrong person, or been tempted by a realistic phishing email. But when sensitive data is involved an innocent mistake can become a costly fine. Sophos Phish Threat tests and trains user to spot and report phishing emails across a wide range of industries and languages.

Sophos SafeGuard delivers file-level encryption, so even if documents are mistakenly sent outside of your corporate network they are unreadable and unusable.

Sophos Central Endpoint Advanced provides data-loss prevention on your endpoint devices. Stop files containing specific keywords or certain file types from leaving the device with preconfigured or custom rules.
GDPR: Understanding the Data Protection Requirements and How to Comply

For several years, high-profile data breaches have been hitting the headlines with alarming regularity. Under the GDPR, consequences for those involved could have been up to €20m or 4% of annual worldwide turnover, which is significantly higher than previous fines. And it’s important to highlight that it isn’t just big names that are affected, every organization that holds data on EU citizens has to comply with the regulation.

Ensuring the confidentiality and security of customer data is paramount to achieving this. Sophos provides encryption, anti-malware and data protection technologies to help your organization meet the requirements of the GDPR.

Appendix

4. 2017 Data Breaches - Privacy Rights Clearinghouse

Try it for free
Register for a free trial at sophos.com/free-trials

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry’s lowest total cost of ownership. Sophos offers award-winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs — a global network of threat intelligence centers. Read more at www.sophos.com/products.