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 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. This whitepaper discusses what the new EU-wide General Data Protection Regulation reform proposals will mean to companies globally.
The Reformed EU Data Protection Laws: Understanding the Data Confidentiality Requirements and How to Comply

Like the majority of states in the U.S., many countries in the European Union (EU) have implemented their own data protection legislation to reflect this new reality of the dissolving network perimeter. As with the differences between US states, the European data protection regulations vary widely from country to country. This, paired with the proliferation of data across new media and technologies, is driving the need to modernize and homogenize the EU Data Protection regulations.

For two years the EU has been working on new Data Protection Regulation reform proposals that will set a Union-wide framework to replace the existing patchwork of country-specific legislation. It 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. At the time of writing, the proposals consist of 91 articles. Like any piece of legislation, the pending Data Protection Regulation reform can be confusing. Our goal with this whitepaper is not to educate readers on the whole of the law but instead to focus on the need to protect the confidentiality of data, which falls under the most severe set of proposed fines. To learn more about the reform effort, please visit the resources listed in the appendix of this document.

Core Elements of Reform

The General Data Protection Regulations reform proposals set a new record with 3,999 amendments on its journey toward becoming a law. After the lengthy review process, the European Parliament demonstrated strong support for the subject of data protection and the reform in a near-unanimous vote of 621 votes in favor, 10 against and 22 abstentions in March 2014. Even though it now has to go through a new round of review and approval process with the Council of the European Union, it is likely that the future legislation will be similar to the proposals we see today.

Here are some examples of what the proposal says about protecting sensitive data.

Article 30 addresses the security of processing data:

1. The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing, taking into account the results of a data protection impact assessment (pursuant to Article 33), having regard to the state of the art and the costs of their implementation.

1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:
   (a) the ability to ensure that the integrity of the personal data is validated;
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
   (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident...

2. The measures referred to in paragraph 1 shall at least:
   (a) ensure that personal data can be accessed only by authorized personnel for legally authorized purposes;
The Reformed EU Data Protection Laws: Understanding the Data Confidentiality Requirements and How to Comply

(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure;
and
(c) ensure the implementation of a security policy with respect to the processing of personal data.

Put simply, the article requires organizations to implement state-of-the-art technical controls that protect data. The article does not specify the technologies that should be used for those controls, but does reserve in a third paragraph the right for a “European Data Protection Board” to specify at a future time “what constitutes state of the art, for specific sectors and in specific data processing situations”.

Should a data breach occur, Article 316 of the proposals specifies that the company is required to immediately notify the supervisory authority. However, the company may or may not be required to notify individuals whose data was breached. Article 327 states:

1. When the personal data breach is likely to adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. (...)

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it.

If, at the time of the loss, the data was protected in such a way as to be unintelligible (and therefore useless to an unauthorized party) – and the company can prove this to the supervisory authority, then the company is not required to disclose the breach to the individuals whose 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 data breach, where appropriate – then the Article 798 on Administrative sanctions stipulates that the supervisory authority can impose at least one of the following sanctions:

a) a warning in writing in the case of first and/or non-intentional non-compliance
b) regular periodic data protection audits
c) a fine up to EUR 100,000,000 or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher.

To summarize: If you don’t put the right technology in place to protect sensitive 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.
Adoption Process for the Proposal to Become Law

The process of enacting a Union-wide law is a lengthy one that can take several years. All three European Union institutions – the European Commission, the European Parliament and the Council of the European Union – must agree on the legislation before it can become active law. The process is driven by the European Commission, which is also responsible for proposing new legislation. In the European Parliament, legislative work on information exchange and data protection is led by the Committee for Civil Liberties, Justice and Home Affairs (LIBE). In the Council of the European Union (also called Council of Ministers), that responsibility falls to the working group DAPIX.

The reformed Data Protection Laws were proposed and amended by the European Commission. In October 2013, the LIBE Committee backed the amended project by an overwhelming majority and received the mandate to negotiate with the Council of the European Union. This vote was then confirmed by the European Parliament in plenary session on 12 March 2014, again by an overwhelming majority of 621 votes in favor, 10 against and 22 abstentions. While European Elections will certainly introduce delays and uncertainties, the amount of legislative work already invested and the near-unanimous vote in favor of this text across all nationalities and political ideologies are indications that this proposal is here to stay and that the momentum will continue. The legislation proposal can now take one of several paths before it becomes law, which might require over a year to go through all the possible steps.
The Reformed EU Data Protection Laws: Understanding the Data Confidentiality Requirements and How to Comply

Who is Impacted by the New Reform?

The status of the EU Data Protection Regulation Reform proposals 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 EU Data Protection Regulation Reform will be:

- One continent, 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 applies 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 New Legislation

For the many companies that must comply with the suggested Data Protection Regulation reform legislation, the best way to prepare is to implement a solid data protection strategy and process that should include encryption in order to be most efficient.

As previously mentioned, the proposed legislation does not require a specific type of technical control other than that it must be “state of the art” and render customer data unintelligible. Thus, it is best to look at how organizations achieve compliance with other regulations that seek to protect sensitive 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 reform proposals. 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 that’s the crux of data protection laws and regulations.

Bottom line: If you want to be ready for the Data Protection Regulation reform, you should start looking at encryption technologies.
How Sophos SafeGuard Helps You Meet the Data Protection Challenge

Adoption of encryption technology has largely been driven by the need to comply with legal and regulatory requirements. However, encryption-adopting companies often have concerns about the technology. Encryption is traditionally perceived as a resource hog that strains IT and hampers user productivity. Older encryption technologies can slow boot up time and annoy users. Others don’t work on the latest hardware or incapacitate machines, and inevitably require time from IT, which is already in high demand.

**Sophos SafeGuard Encryption** provides encryption without compromise. Modern versions of Windows and Mac operating systems come with built-in encryption engines. SafeGuard leverages these native OS encryption engines whenever possible to reduce the impact on the end user. The result is protection plus performance.

We also make encryption simple by protecting all machines across all platforms without getting in the way of users and how they want to work. SafeGuard follows data to protect it everywhere. Whether in the cloud, on removable storage devices, in network files, or on mobile devices – SafeGuard goes wherever your data goes.

Keeping encryption simple also means making it easy for IT to roll out and manage. Auditing and reporting capabilities support compliance efforts, enabling IT to prove that a file, machine or USB stick was encrypted at the time it was lost, stolen or breached. All of these features bring peace of mind to companies that risk high fines if found to be out of compliance with data protection laws.

Only Sophos gives you encryption for your users’ computers, their shared folders, removable media and data stored in the cloud, both for Windows and Mac. And you get all this versatility from a single agent and management console. Our certified encryption stops data breaches and makes compliance simpler without getting in your way. Plus you save time because our data protection is easy to manage.

Conclusion

With fear of government surveillance coupled with news of high profile data breaches in the media, the pressure and requirements to protect sensitive customer data is increasing. Meanwhile, customer confidence in business is eroding. European Parliament, data protection authorities and governments want to help safeguard and boost the European online economy meaning that many companies will need to implement processes and technical controls to ensure the confidentiality of customer data.

Encryption should be part of this solution, as it will prevent unauthorized users from reading data if it is lost or stolen. **Sophos SafeGuard Encryption** ensures that companies get the protection they require without impacting user workflow or draining IT resources.
Appendix

1. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). European Commission, 25 January 2012.


See how it works
Learn how SafeGuard Encryption can help your company comply with data protection regulations at sophos.com/encryption

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