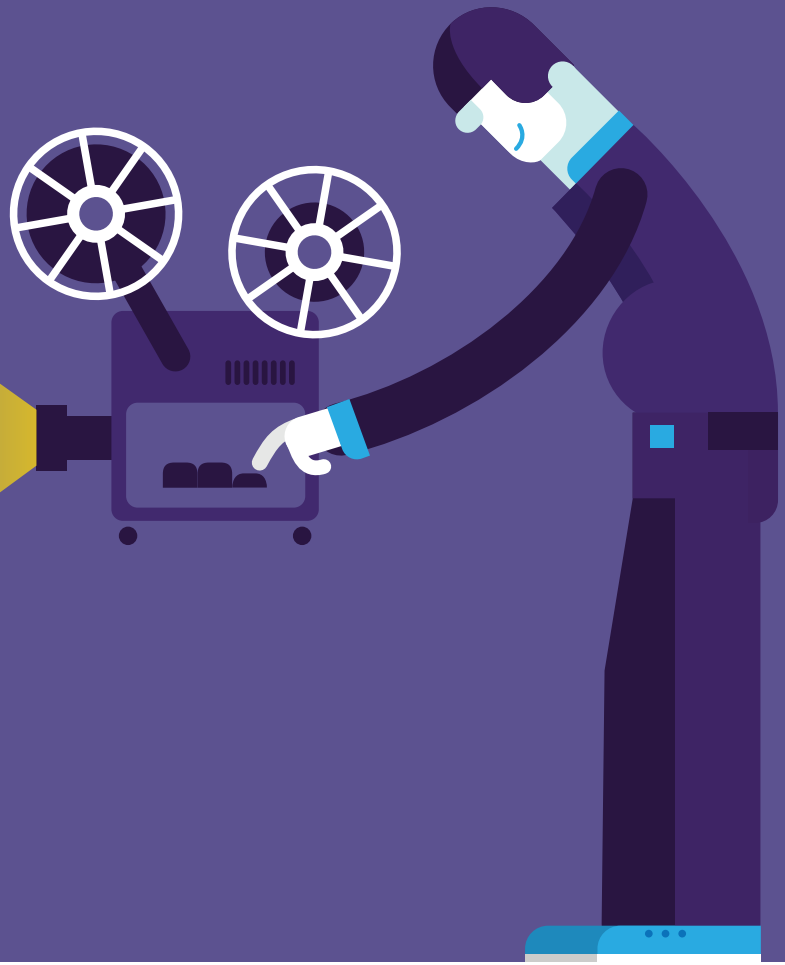
www.**infinity**.bg

The road to **GDPR compliance**



ENDPOINT PROTECTOR | by CoSoSys

www.**endpointprotector**.com

The road to **GDPR compliance**

Table of Contents

1 What is GDPR

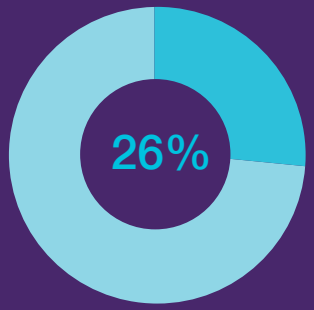
The EU General Data Protection Regulation (GDPR) is a regulation issued by the European Commission, the European Parliament and the Council of Ministers of the European Union with the purpose of strengthening and unifying data protection for individuals within the European Union. It is the most important change in data privacy regulation in 20 years, according to the GDPR portal. It took four years of preparation and debate until it was finally approved by the EU Parliament on 14 April 2016.

The General Data Protection (GDPR) regulation makes a big statement about individuals' private data and their right to request data controllers and processors to delete, correct, and forward their data. In consequence, GDPR comes with significant changes compared to the Data Protection Directive 95/46/EC involving operational changes in organizations. These will impose stricter fines in case of failing to protect EU citizens properly.

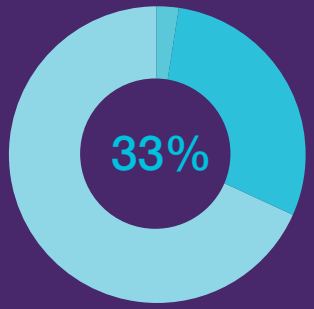
1.1 GDPR readiness

Organizations have started to feel the pressure because the day when the law will come into effect is fast approaching. Many of them are far from being close to GDPR compliance and the changes they have to apply require a great effort on all levels of the business. In fact, at the end of 2016, a survey conducted by AvePoint on 223 respondents from multinational organizations revealed that only 26 percent of them keep records of data processing and transfers, only 33 percent classify data and only 10 percent of those use automatic data classification. The percentages are concerning as all of these are essential requirements of the GDPR. The study also showed that companies are in different stages of preparation for the upcoming regulation, with slow progress. For example, some have appointed a DPO, while others are still assessing the impact of GDPR on their operations.

This whitepaper's purpose is to help take some of the pressure off for organizations, by offering guidelines on operational tactics for the preparation for GDPR.



Only 26 percent of organizations keep records of data processing and transfers



Only 33 percent classify data and only 10 percent of those use automatic data classification

Have you sketched a game plan yet?

1.2 Key articles and how they impact businesses

Extended jurisdiction

GDPR is clearly defining the territorial applicability, stating that it applies to all organizations collecting and processing personal data of individuals residing in the EU, regardless of the company location, so it doesn't matter if the processing takes place in the European Union or not. For example, a company with the HQ in the USA, offering goods or services to EU citizens, falls under the GDPR jurisdiction.

Consent

No more evasive consent notices. All organizations will be obliged to obtain the individuals' consent to store and use their data and they must explain how it is used. At any time after the regulation comes into effect, data collectors must be able to prove that consent has been obtained. For individuals, it will be easier to withdraw their approval.

Mandatory breach notification

Companies are obliged to notify the supervisory authority within 72 hours of discovering the breach unless the breach is unlikely to "result in a risk to the rights and freedom of individuals." The notification has to include specific information about the nature of the data breach, the number, and type of breached records, the name of the Data Protection Officer, the measures taken to mitigate the risks, and other details.

Right to access

This article is a great foundation towards transparency, giving individuals the right to request information from organizations about what personal data concerning them they are processing, where it is stored, and for what purpose. Companies must be able to provide a copy of people's private records in electronic format.

Right to be forgotten

Also called 'right to erasure', this article empowers EU citizens to request the controller to delete their personal data and, further than this, to stop sharing it with third parties, which are also obliged to stop processing it. Article 17 for the GDPR includes a list of situations when the right to be forgotten applies: personal data is no longer necessary in relation to the purposes for which it was collected or processed, the individual withdraws consent, the data has been unlawfully processed, and others.

Data portability

In case an individual wants to transmit his / her data from one controller to another, this article of the GDPR gives him/her the right and the framework to do so. Therefore, organizations must be able to provide personal data in a 'commonly use and machine readable format' if requested by individuals.

Privacy by design

Just like 'security by design', privacy by design refers to including information security in all processes, systems, products or services from the start, resulting in strong, consistent data protection implementations and avoiding loopholes caused by security additions further down the line. The key here is that privacy by design is a legal requirement with the GDPR, not just a recommendation.

Data Protection Officers

Both data controllers and data processors are required to appoint a Data Protection Officer. Who can take the role of the DPO and what he/she is responsible for are detailed in Articles 37 to 39 of the GDPR. In short, the DPO can be a member of the organization's staff or can be contracted for services. NOT all companies are obliged to have a DPO, but only those "controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offenses," according to EUGDPR.org. The DPO's main responsibilities are to ensure the application of the GDPR, to keep a register of the processing operations involving private data, to provide advice and inform collectors and processors of their obligations derived from GDPR.

1.3 Penalties

Depending on the nature, gravity, duration of the infringement, the number of the data subjects affected and the level of damaged and several other factors, penalties are:

Up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

Up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

2. Two cornerstones in the process of becoming GDPR compliant

To be able to apply the enhanced, stricter rules, organizations should perform an audit to their current data security solutions and processes implementation and build upon it. The audit should reveal what data is collected from individuals, if there are proper consent procedures, where are private details stored, who has access to them, how is the integrity of private data ensured, etc. Based on the discovered pieces of information, a solid plan for upgrading to the new regulation can be outlined and shared with all involved parties. Let's see how the game plan would look like in order to maximize your chances of getting to the finish line without spending too many resources.

Awareness

Chief Security Officers, IT Managers, CEOs, business unit managers, etc. have to be informed of the legal changes the GDPR imposes and should make sure they translate them into plain, simple measures to apply in order to respect this regulation. The clearer the objectives are, the sooner everyone will understand what their role is and act accordingly. All department managers, top managers, and other decision makers should carefully read the GDPR, or get advice from a lawyer regarding the obligations stated in the regulation. The terminology used in this kind of regulations is usually difficult to understand, so asking for a lawyer's advice is recommended, if not mandatory. Having full awareness of a company's obligations concerning private data protection represents a solid foundation for the next steps.

Treat the GDPR compliance as a project, where the initiation and planning phase are defining.

Get advice from a lawyer.

Disciplined execution

The strategy is worth nothing without a disciplined execution. Knowing what data security and management solutions have to be selected and implemented to ensure compliance and security is not as easy as it would seem. There are numerous factors that weigh in and the human factor is the most complex. A simple example would be the Data Protection Officer that has to be appointed. Companies have a tough decision to make, considering the level of responsibility assigned to a DPO. The officer has to make sure that data protection compliance is met, so his / her role is crucial and difficult, having to deal with employees on one side and departments' managers on the other side.

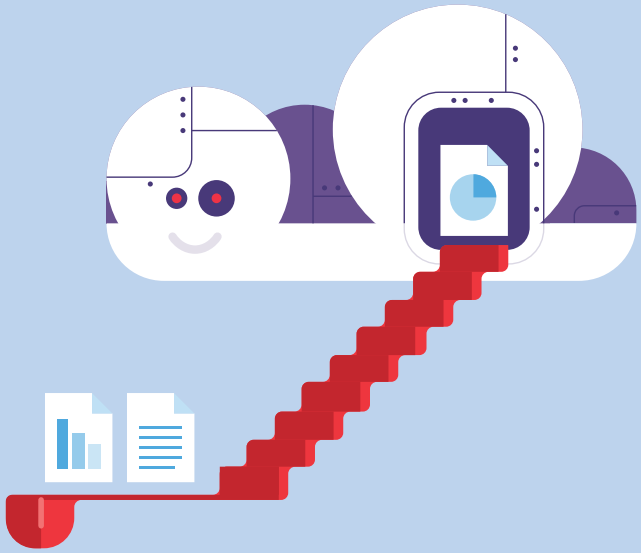
Also difficult to execute is the article referring to the cross-borders transfers which extend farther than physical borders where the headquarter or branches of a company are. A company operating in Germany can have customers in France, USA or any other country. This comes with a big responsibility in what concerns individuals' data security. The GDPR will apply to the processing of personal data of individuals residing in the EU, even if the controller or processor is not located in the EU. So, if your business is not in the European Union, you can still be subject to this regulation.

Your assignment is to identify what data you store and process for European citizens, its location, its path from point A to B, by what systems is it processed, etc. Doing that, you can further realize if you have the required tools to protect private data, or what tools you may need to support you in achieving GDPR compliance.

A real game-changer will be the 'data protection by design and by default' principle. This will require services or products to include privacy and security features from the very beginning of concept and development. That should be interesting especially for mobile app developers and the IoT sector. The new regulation will be a great motivator for vendors to align data security with innovation and build not only ingenious products but also secure products.

Beyond the product or service reference, the privacy by design principle should be applied also to processes, according to the GDPR rules. Basically, for any organizational process, whether it is operational, logistic, internal communication, HR, and any other process involving private data, the companies must take into consideration security as a pillar with the same importance as any other element. As an example, when creating an HR department, besides determining the required number of people, responsibilities, procedures, a business should establish the privacy policy and how it is achieved as well.

3. How Endpoint Protector solutions help you get faster to GDPR compliance



From planning to execution, software accompanied by the intervention of key people's insights helps businesses to efficiently apply the necessary changes for the readiness with the new regulation. So, how can we help specifically with our DLP solution in your quest to become compliant with GDPR?

The audit

An important part of the audit is covered by Endpoint Protector Data Loss Prevention. In the initial phases of the GDPR compliance, organizations can use Endpoint Protector DLP with policies set on report only, so data that is being transferred outside the company is being tracked and reported. Businesses can get valuable insights about what users are transferring sensitive data, like personally identifiable information, credit card numbers, social security numbers, and other confidential information.

Additionally, the exit points can be flagged for monitoring, to detect exactly where the confidential data goes – on cloud apps, by e-mail, on portable storage devices, on webmail, etc. The most active users when it comes to data transfers and devices connections can be discovered and based on this information together with data gathered from audit software can paint a picture on the actual situation before moving forward with operational changes for compliance.

Data movement restrictions

Once the audit is finalized, organizations have to strengthen security and address the vulnerabilities. Endpoint Protector monitoring policies can be converted into restrictive policies, blocking unwanted file transfers, unauthorized data copied/pasted, screen captures, etc. and all of this depending on the various transfer channels and the users, computers, groups that are part of the organizational structure. Since individuals' private data is so crucial to protect according to the updated regulation, it can be secured against leakages and theft with the content filtering capabilities available in Endpoint Protector DLP.

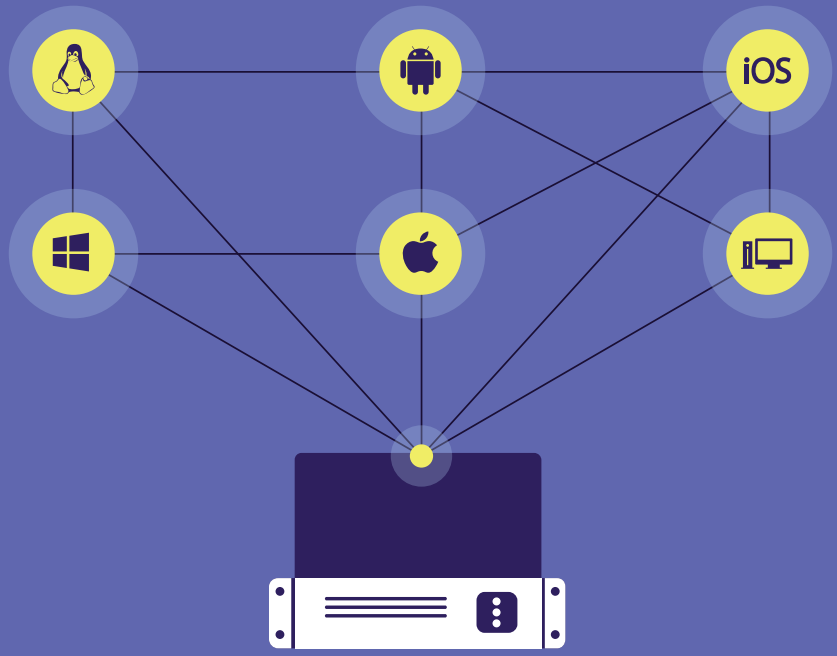
Our solution can also help in the cross-border data transfers. Organizations are prohibited from transferring personal data to recipients outside the EEA, unless the region of destination provides an adequate level of data protection (deemed by the European Commission), or unless there are other circumstances set also by the European Commission. This scenario applies to companies using online IT services, multinational companies with several establishments in the EU Member States, cloud-based services, remote access services, and other similar business models. Endpoint Protector can detect and block data transfers to solutions with data centers located in countries outside the EU (e.g. Dropbox) or, in case those countries fit in the adequacy level of data protection, data transfers can be allowed. It all comes down to the control you get for sensitive data movement.

Another helpful aspect is Endpoint Protector architecture that allows the management of the web console from one country and the computers being managed for DLP in another country. This flexibility makes tracking and blocking of data transfers achievable regardless of the business location, so multi-establishment organizations can implement one solution for all their offices.

3. How Endpoint Protector solutions help you get faster to GDPR compliance

Multiple layers protection

The GDPR states that data privacy should be ensured, with no specifics about the platform, if it is Windows, macOS or Linux, iOS, Android, Windows Phone, etc. or the exit channels – e-mail, file cloud sharing, removable devices, etc. It is not important, after all. The essential part is that data must be secured no matter what. Therefore, for any data security tool you choose to implement, make sure it covers your entire infrastructure, all endpoints, mobile devices, exit points.



Endpoint Protector DLP helps you protect sensitive private information against data loss and theft on Windows, macOS, and Linux, while the Endpoint Protector Mobile Device Management solution, included in the same management interface as the DLP solution, secures data on iOS and Android devices as well as macOS computers.

4. Compliance with GDPR cuts costs

The General Data Protection Regulation can cause serious headaches until full compliance is achieved, but after that milestone, organizations will be able to see how the benefits outweigh the efforts. Entering new markets in Europe will be easier for businesses because the data protection regulation will be the same as in their home country. The European Commission exemplifies in a press release how companies can cut costs thanks to the reform.

Example: Cutting costs
A chain of shops has its head office in France and franchised shops in 14 other EU countries. Each shop collects data relating to clients and transfers it to the head office in France for further processing.

With the current rules: *France's data protection laws would apply to the processing done by the head office, but individual shops would still have to report to their national data protection authority, to confirm they were processing data in accordance with national laws in the country where they were located. This means the company's head office would have to consult local lawyers for all its branches to ensure compliance with the law. The total costs arising from reporting requirements in all countries could be over €12,000.*

With the Data Protection Reform:
The data protection law across all 14 EU countries will be the same – one European Union – one law. This will eliminate the need to consult with local lawyers to ensure local compliance for the franchised shops. The result is direct cost savings and legal certainty.

5. Conclusions

GDPR is causing a lot of noise among businesses, especially European ones. Many are not yet sure in what position they are, if they are a controller or processor. Many companies are delaying the initiation of becoming compliant being overwhelmed by the necessary changes and others are simply not aware of the implications.

Regardless of what position you find yourself in, in May 2018 everything has to be in place and starting with that moment you have to be able to prove at anytime you are compliant and that you securely conduct your activity without endangering the privacy of your employees, customers, partners, and other stakeholders.

If you haven't started working on GDPR compliance, awareness across business units is the first thing to achieve, followed by a sound audit and a great execution. Choose carefully what software can help you in each stage of the process and always complement software implementation with the particularities of your organization, the legal framework and the human factor.

References:

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
http://www.eugdpr.org/key-changes.html
http://www.cmswire.com/information-management/how-businesses-are-preparing-for-the-gdpr/
https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/
http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

www.**infinity**.bg

ENDPOINT PROTECTOR | by CoSoSys

www.**endpointprotector**.com

Germany

E-mail vertrieb@endpointprotector.de
Phone +49 7541 978 26730

United Arab Emirates

E-mail me@endpointprotector.com
Phone +9714 3699768

Romania (HQ)

info@cososys.com
+40-264-593 110

South Korea

support@cososys.co.kr
+82 70-4633-0353

Bulgaria

Infinity Ltd.
+359 2 489 02 59
+359 884 166118
office@infinity.bg
www.infinity.bg

COSOSYS