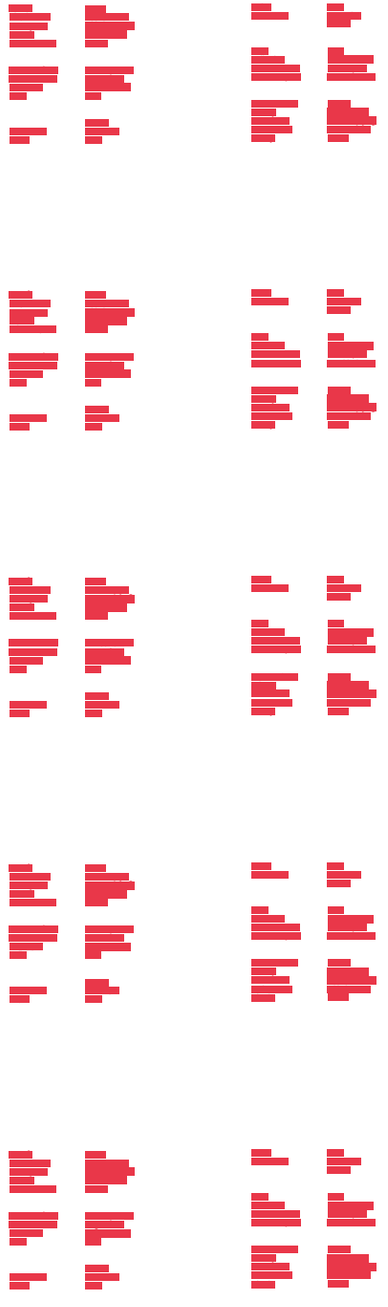
EU GDPR

Compliance Checklist

10 Steps to Compliance



Have you been making preparations for the new General Data Protection Regulation?

The GDPR will come into effect in **May 2018**, and will apply directly to all European Union citizens and companies. Studies have shown that most of organizations aren't GDPR compliant yet, despite being familiar with the Regulation.

The lack of preparedness for the GDPR will have an impact on everyone, as organizations and businesses run the risk of receiving penalties as a consequence of cyber security breaches. Thus, it's essential to approach this topic with rigour and to follow the set of mandatory guidelines required by the European Union.

To help you kick off the preparation process and support you in achieving GDPR compliance, we have gathered a checklist that includes the steps you need to take. At the end you'll also find a generous list of resources and examples you can adapt and use for your own organization.

Raise Awareness

Given the increasingly data-driven world, the new Regulation is aimed at giving EU citizens more control over their personal data. By May 2018, all decision makers and key persons within a company should be aware of the new legislation, understand the reasons for compliance, or how to collect and process data.

Compliance should be a serious focus for organizations that need to inform its employees about the privacy issues, and be proactive.

Conduct a Data Audit

Organizations should conduct a data audit for all the personal data they're collecting and demonstrate how they comply with the new GDPR. This means that every organization needs to organize and record the processing activities: what personal data it's holding, where it is being kept and who it's being shared with.

Communicate Privacy Information and Consent Clearly

The new regulation has tightened the conditions for consent, meaning that organizations need to have explicit consent when they are collecting data about their customers.

The GDPR specifies that "*consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language.*" Each time an organization processes sensitive data, it has to inform customers about the way their data are being used.

Customers can withdraw consent at any time, and systems must be able to handle these withdrawal requests.

Data Collection Rules Become More Compact

The new Regulation requires organizations to justify **what** information they process and collect about their customers, including purposes of processing their data.

"*Persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.*", says the **law**.

Users have the right to complain and get redress, if data is misused anywhere within the European Union.

Individuals Have More Extensive Rights

Individuals have much broader rights under the new Data Protection Regulation.

They are entitled to:

- Require to erase outdated data (“right to be forgotten”)
- Transfer personal data from one electronic system to another (data portability)
- Correct inaccurate personal data
- Have more control over how their data is used
- Launch a lawsuit in the event of a data breach or other events that put their personal information at risk.

Data Breaches New Procedure

According to the new regulation, organizations that manage personal data are required to quickly notify the authorities in case of a data breach without delay. And “without undue delay” is translated into **72 hours**.

Data Protection Officer

The new GDPR also requires organizations that process more than 5000 data subjects in a 12 month period to have a Data Protection Officer (DPO).

Here is what a DPO should do:

- Be proficient at managing IT processes and resources;
- Educate organizations and employees on compliance issues;
- Serve as a liaison between an organization and GDPR authorities;
- Keep record of all data processing activities organized by an organization.

New Regulation on Data Export Outside the EU

The new legislation states that personal data can only be transferred to countries outside the EU and the EEA (European Economic Area) when an adequate level of protection is guaranteed.

Severe Penalties for Not Complying with the New GDPR

For those who don't comply with the new GDPR, the European Commission introduced severe penalties to be applied:

- A warning in writing in cases of first and non-intentional non-compliance
- Data Protection Audits
- **Fines up to €20 million or 4 % of annual global turnover** of the organization at fault.

Data Protection by Design and Default

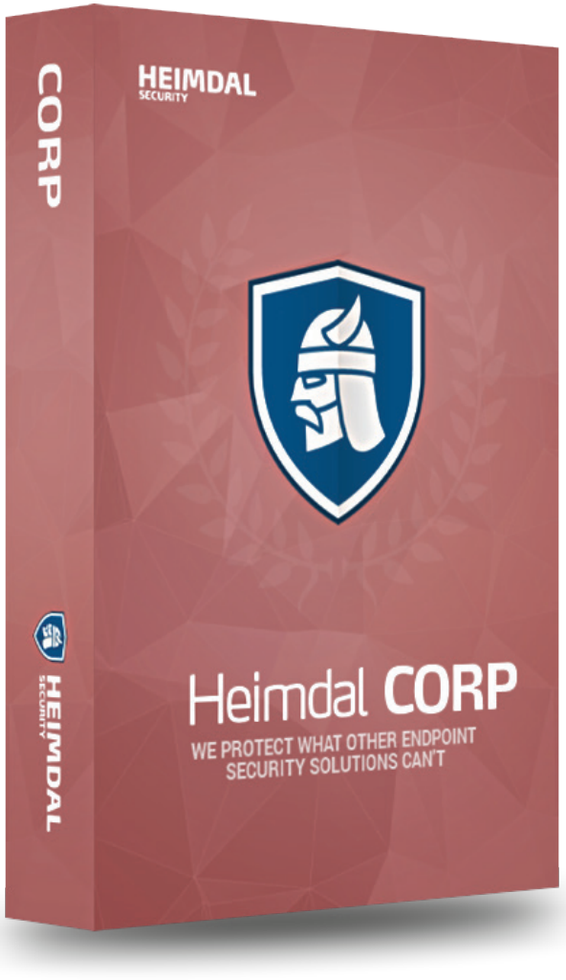
The new Regulation requires organizations to consider data protection requirements when new technologies are designed.

Remember that the new DGPR will come into effect in **May 2018!**

With only a few months left to prepare, you should know that **Heimdal CORP** can help you strengthen your organization's security, while also helping you achieve GDPR compliance and save time.

Here are some of the way that Heimdal CORP can help:

- Provides real-time threat and status reporting, delivered in intervals of your choosing
- Helps prevent data leaks (DLP) by blocking data transfers to cybercriminals' infrastructure



- Stores the entire history as long as you are a customer (a huge help in compliance audits)
- Assesses and prevents the risk of infection (IDP/HIPS), because it's able to find infections that no other solutions can detect
- Saves time and effort by automating patching and matching your requires conditions for silent and automatic deployment of patches and more!

CLICK TO READ MORE

Our **security consultants** can help you see if Heimdal CORP is a good fit for your needs and provide more details about the product, as well as help you set up a FREE DEMO.

Andreea **Botezatu**

www.heimdalsecurity.com

abo@heimdalsecurity.com

+40 726 781 188

Conduct a Data Audit

Data Breaches New Procedure

Raise Awareness

Data Protection Officer

Data Protection by Design and Default

Individuals Have More Extensive Rights

Data Collection Rules Become More Compact

New Regulation on Data Export Outside the EU

Communicate Privacy Information and Consent Clearly

Severe Penalties for Not Complying with the New GDPR

Legislation

Regulation (EU) 2016/679

EU GDPR Portal

Resources

Microsoft's GDPR Tools

Google's Privacy and Security Tools

Google Analytics Solutions

GDPR Self-Assessment Free Tool

Privacy and Data Protection Exam

The International Association of Privacy Professionals

GDPR Infographic

Be Prepared for GDPR (Webinar)

Data Protection Documents (European Commision)

Best Practice Examples

Great Examples of Transparent Data and Privacy Policies Ahead of GDPR

GDPR Report: Most Organizations are Implementing Data Breach Notification Procedures

GDPR Best Practices Implementation Guide

EU GDPR Security Articles

Key Priorities to Prepare for EU GDPR

What Security Pros Need to Know About the New Era of Privacy Regulations

A Primer on GDPR: What You Should Know

What is GDPR? Everything you need to know

Is the World Ready for GDPR? 75 Percent of U.S. Companies Think GDPR Doesn't Apply to Them

10 Things You Need to Know about the New GDPR