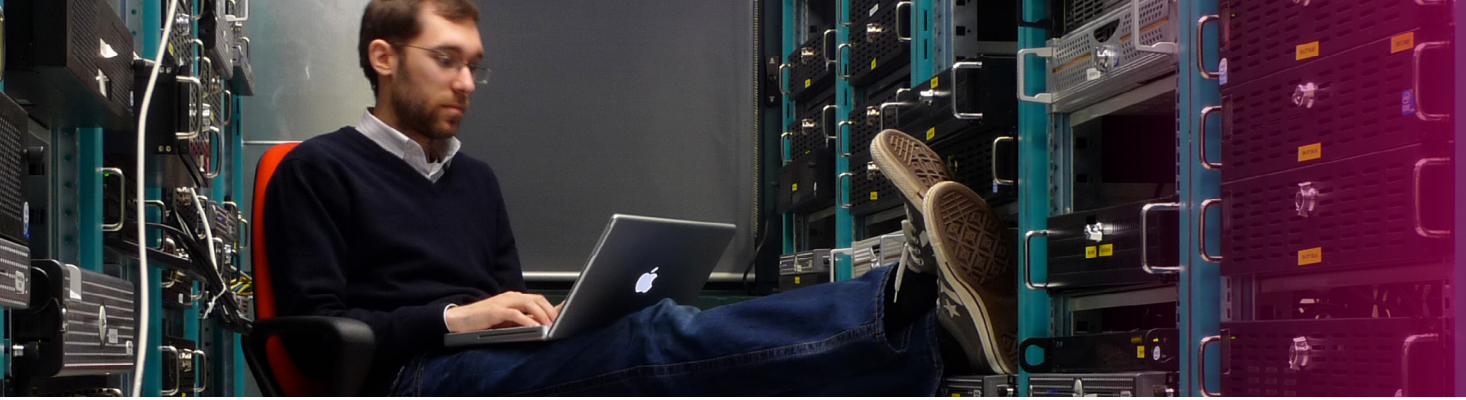

THE GENERAL DATA PROTECTION REGULATION

# With financial penalties of up to 4 percent of global annual turnover, are you up-to-date on the General Data Protection Regulation?



**The primary objectives of the GDPR are to strengthen and harmonize data protection for individuals as well as simplify the regulatory environment for businesses.**

**THE WORLD** has come a long way in terms of technological progress since the initial implementation of the current EU Data Protection Directive (95/46/EC). This progress has profoundly altered the way personal identifiable information (PII) is collected, accessed, and utilized.

On January 25 2012, in order to strengthen individual privacy rights, the European Commission proposed a comprehensive reform of the old EU Data Protection Directive – and on 27 April 2016 a new regulation, known as the GDPR, was adopted. It enters into application on 25 May 2018 after a two-year transition period.

This document details the effects of General Data Protection Regulation (GDPR) and aims to provide an explanation of the amount of preparation involved for organizations in adapting to these changes.

## What is the General Data Protection Regulation?

The GDPR contains a number of requirements on how organizations should process and safeguard personal identifiable information of individuals residing in the European Union.

The regulation also addresses export of personal identifiable information outside the EU and will replace the Data Protection Directive (95/46/EC) from 1995.

It is important to note that there is a new Directive in addition to the GDPR. The Directive will apply to policy procedures, which will continue to vary between EU member states. This document will not go into details on the Directive.

## Scope of the Regulation

The GDPR will apply if organizations process data of individuals based in the EU.

In accordance with the current Data Protection Directive, European organizations have to adhere to much stricter standards than organizations outside the EU – with GDPR, organizations based outside the EU must adhere to the same rules as European-based companies if they process personal identifiable information of EU residents.

According to the European Commission personal identifiable information is defined as:

*"any information relating to an individual, whether it relates to his*

**The GDPR applies to all organizations processing personal identifiable information – both located in- and outside the EU.**


**LogPoint is the only European EAL3+ certified SIEM solution. This certification testifies that the LogPoint software is secure on one of the highest levels possible. This means LogPoint can be utilized worldwide by NATO organizations, law enforcement, military and critical infrastructure providers.**

*or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."*

## What is Included?

GDPR introduces several new actions concerning how data is collected, stored, accessed and utilized and details how companies are obliged to respond in the event of a data breach. It contains the following key points:

**Consent:** Individuals must provide specific, informed and unequivocal consent for processing of their information collected for specific purposes. Valid consent must be explicit for the data collected and the purposes used - and consent may be withdrawn. It is required that organizations are able to prove consent for 'sensitive' data.

**Data Protection Officer (DPO):** When the regulation enters into force, all public institutions will be required to employ a DPO. All private organizations must also employ a DPO, if their business centers on processing personal identifiable information or systematic monitoring of a number of people. Despite whether a DPO is required, all businesses must be able to document that they are in control of security concerning personal identifiable information.

**Data Breaches:** The data controller will be obliged to notify the relevant supervisory authorities without "undue delay" in the case of a data breach and where feasible, no later than 72 hours after having become aware of a breach. This does not apply if the "breach is unlikely to result in a risk for the rights and freedoms individuals." Individuals whose data have been breached have to be notified if undesirable impact is determined – that is, if there is a high risk to the rights and freedoms of individuals.

**Right to Erasure:** Replaces the so-called 'right to be forgotten' and signifies that individuals have the right to request removal of personal identifiable information on any one of a number of grounds such as if the data is no longer needed for the collected purpose or if the individual withdraws their consent.

**Data Portability:** The GDPR outlines that individuals must be able to transfer their data from one processor to another, and the data must be presented in a structured, commonly used electronic format. This is implemented e.g. to ensure individuals are protected from having their data stored on closed platforms, where they are subject to lock in.

## Why Does it Matter to My Organization?

The current Directive is implemented differently in all EU member countries. With the GDPR there will be only one single, pan-European regulation for data protection – although (with country specific variations).

LogPoint · Email: info@logpoint.com · Telephone: +45 7060 6100

logpoint

**Non-compliance can result in financial penalties of 4 % of an organization's global annual turnover or 20 million Euro, whichever is greater.**

The fact that it is a regulation instead of a directive means it will be directly applicable to all EU member states.

It is of crucial importance that organizations seriously consider how to ensure compliance to the GDPR, as the effects of non-compliance means severe financial penalties. These penalties will be determined based on the extent of the data leakage, and a two-tiered sactions system will apply.

Some breaches, which have been deemed by law makers to be key for data protection, may constitute fines of up to 4 % of a organization's global annual turnover or 20 million Euro for the preceding financial year, whichever is greater. Other breaches may result in fines of up to 10 million Euro or 2 % of global annual turnover. Further, individuals whose data have been breached are able to potentially file lawsuits for compensation in parallel with these financial penalties.

## How We Can Help

At LogPoint, we have already experienced considerable interest in the effects the new regulation will have on organizations.

We suggest a thorough review of your security and data protection policies as well as roles and responsibilities within your organization. Further, a risk assessment and action plan for dealing with the inherent risks within your organization should also be a priority.

LogPoint can assist your organization in complying with this new standard. By utilizing our SIEM solution, you are able to monitor access to systems where personal identifiable information is stored as well as monitor the security on those systems and receive alerts when they are accessed.

A thoroughly implemented SIEM installation will ensure that logs exist, are stored and protected, while the processes around the SIEM will ensure that alerts, incidents and reports are processed in due time.

Implementation of the regulation may seem far away, yet experience shows that considering the actual review of the organizational setup as well as potential system upgrades, process changes and new implementations, starting the process now would not be a day too soon.

We are experts in assisting organizations with their security and compliance requirements. Please feel free to contact us, if you would like additional information.

LogPoint · Email: info@logpoint.com · Telephone: +45 7060 6100

logpoint