STEALTHbits TECHNOLOGIES

CAS Severn

5 Essential Steps to EU GDPR Compliance: Part 1

Understand the Basic Requirements of GDPR

Source: The Insider Threat Security Blog

Part 1: Understand the Basic Requirements of GDPR

Despite the GDPR being marked as a clearer to understand regulation, it's still a mine field of legal and compliance requirements, interpretations and uncertainty.

The purpose of this blog series is to help you understand the fundamental requirements of GDPR by peeling back the layers of legality, bureaucracy and spin.

The Numbers

It's safe to say that the numbers have stolen all of the GDPR headlines:

- 4% of global revenue or €20m fines
- 72 hours to notify the regulatory body upon discovering a data breach

Let's put some context around these figures, based on existing Data Protection (DP) regulations.

In the UK, under the Data Protection act of 1995 the maximum an organization can be fined is £500k.

While £500k may be a lot to SMB organizations, to a global enterprise it's a risk worth taking versus investing millions in Data Protection.

Currently in the US, organizations have 90 days to notify of a data breach.

In realistic terms, it means that if a breach is discovered on a Friday, the organization will need to work across the weekend to gather all of the required information to ensure they meet the notification deadline.

The Questions

Data Subject Access Requests (DSAR)

The premise behind the EU GDPR is to guarantee the fundamental right of an EU Citizen to privacy and enforce the right of erasure.

Organizations will need to be able to respond to a DSAR, with common questions likely to be along the lines of:

'Do you hold any of my data'

'What is that data'

'Please delete my data'

'Please provide my data in a format that can be transferred'

'Is my data secure'

As simple as these questions may appear, the ability to respond to them is anything but simple.

The Challenge

Imagine for a moment that you had to provide answers to the above questions for a single person right now.

Can you do the following:

- Stipulate exactly what criteria constitutes personal data and then identify it
- State exactly what that data is and what it is used for
- Determine what can and should be deleted
- Extract the required data and supply to the data subject
- Prove that you have done everything to ensure the data is secure
- Now, imagine you are asked to do this for 10 data subjects, 100 data subjects, 1,000 data subjects.
- The scale of task becomes apparent and this is before you add the layers of legality and regulation.