STEALTHbits TECHNOLOGIES

CAS Severn

5 Essential Steps to EU GDPR Compliance: Part 4

STEALTHbits Technologies, a Logical Fit for EU GDPR

Source: The Insider Threat Security Blog

In part three we discussed how no one person, organization or vendor has 'the' silver bullet to GDPR compliance. What you need is an array of tools and people to address the many challenges ahead.

Saying that not all technical solutions are equal in their value to a GDPR project. Given GDPR is a Data Governance project (as discussed in part two), it makes sense to leverage both technology and people with Data Governance running through their veins

STEALTHbits is that.

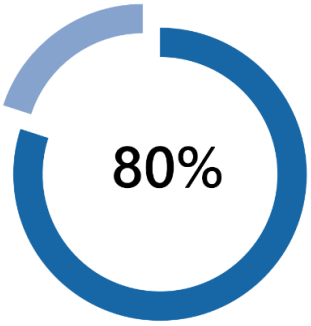
STEALTHbits has focused on Data Governance for 16 years, focusing on being the best at providing a global leading Data Access Governance platform for unstructured data.

We have a comprehensive breakdown of articles and chapters along with a functionality and report mapping. The detail is far too much for a blog so please contact your local STEALTHbits representative who can provide you with this. For quick reference, here's an outline:

EU GDPR Article Alignment

For the full infographic with detailed explanations of each section, please follow this link: https://www.stealthbits.com/preparing-for-the-eu-gdpr-time-bomb

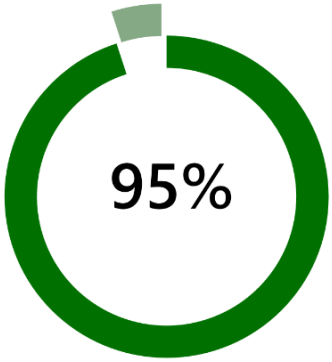
If you look at the high-level requirements of the GDPR as well as the following statistics regarding Data Governance, you can start to see the scale of the challenge ahead if your organization hasn't already undertaken or started a Data Access Governance project.



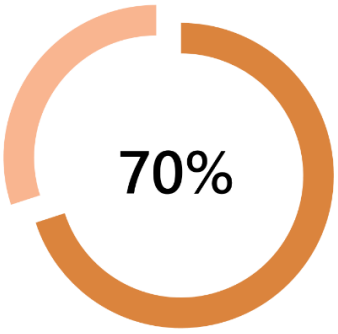
…of Data in organizations is unstructured

This includes file systems, SharePoint, Email, cloud Storage. Anything that isn't stored in a database or application with a set format. Unstructured data is hard to manage and could, in theory, be anywhere in your environment.

…of Organizations use Active Directory as their primary source of Authentication



Your user account and groups that provide access to unstructured and often structured data, is managed by Active Directory. The policies that govern things such as passwords, access levels, name resolution and many other business critical services are also reliant on AD. Active Directory is the foundation of most businesses environment. Lose AD, lose access to data.



…of data has excessive access granted

Put AD and data together, add a pinch of legacy practices and general day to day use and people end up with access to data they shouldn't. That could be the ability to read files they shouldn't or manipulating files they should only read. Either way, this breaks all basic rules of Data Governance and 'Privacy by Design'.

I would say this is a problem in 100% of organizations to some degree.

…for the average data breach to be discovered,

if the breach is discovered at all. Most data breaches are never uncovered. A breach isn't just the headline grabbing incident like Yahoo. It also covers that former employee who takes a document to their new role with them.

Either way, for GDPR it's not so much the discovery that applies to the 72-hour notification period, it's the ability to investigate the 'Who, what, where, when and how' once a breach has been discovered. These findings must then be supplied to the appropriate regulatory authority.

Next week we conclude this series by pulling together elements from each blog to form a strategy for addressing GDPR compliance; understand the challenge, engage the right people/organizations, utilize the right technology and act now.