STEALTHbits TECHNOLOGIES

40 CAS Severn

5 Essential Steps to EU GDPR Compliance: Part 3

Engage the Right People

Source: The Insider Threat Security Blog

This is arguably the most important element in achieving GDPR compliance. No organization can do everything independently. Even software vendors must engage with outside agencies on this one.

We're going to discuss 'the right people' as two categories; Internal and External. If ever there was an all hands requirement in a project, this is it.

Internal

Because GDPR is a compliance regulation, it's far too easy to fall into the trap of believing this is simply a job for the InfoSec team, assisted by the IT guys (isn't everything?). Yes, they are the most likely leaders in this project, but many other internal stakeholders must be included. Let's look at some basic requirements of GDPR again and align to generic business roles and departments.

We'll do this in table format to keep things digestible:

Element	Description	Impacted
Data Capture – Consent	Most organizations don't have this so a new process must be designed and implemented	• Call takers • Helpdesks • Human Resources • Finance • Internal Comms

Data Capture – Recording	The flow of data from receiving through to storage must be documented, transparent and fully auditable	• Call takers • Helpdesks • Human Resources • Finance • Internal Comms • Legal
Data Processing – DSAR	Be able to respond to Data Subject Access Requests	• Helpdesks • Human Resources • Data Analysts • Internal Comms • Legal
Data Processing – Retrieval / Deletion	The right to be forgotten and the necessity to provide data in a format suitable for transport	• Helpdesks • Human Resources • Data Analysts • Internal Comms • Legal
Privacy by Design	Ensuring data is secure	• Arguably everyone in the organization

*Infosec & IT left out as they are a given

I'm not for one second suggesting this is an exhaustive list or that it's 100% accurate. Nor applicable to every organization. It's intended to demonstrate that for each element of End-to-End Data Processing, multiple elements within an organization are involved at each step of the way.

- **Why Human Resources?** They are the ones that must write the internal policies governing that all members of staff adhere to the new processes with enforcing penalties if broken.
- **Why Internal Comms?** Everyone in the organization with any form of responsibility for data must know changes to process with re-percussions of not adhering. This is not uncommon in any project of scale, but Comms teams do often need to be the first to make a start. The last thing any organization needs is for a member of staff to say 'I didn't know…'. Ignorance is no excuse.
- **Why Legal?** If you have a legal team, they must be versed in the Legal responsibilities of organizations that fall within the GDPR remit.

External

There are three things to remember and these are often the topic of conversation among Cyber Security Specialists:

- Currently, there is no such thing as a 'GDPR Specialist'. There can't be until GDPR has been enforced and there are test cases available. However, there are time served Cyber Security Specialists who know GDPR well.

- No one solution or vendor has a silver bullet that will solve all things GDPR. Given the complexities of the regulation and many touch points, it would be impossible for one vendor to cover all elements.
- Many vendors are purporting to have a GDPR solution and/or be GDPR compliant, often they are stretching their capabilities and GDPR requirements to fit. The square peg in a round hole analogy applies here.

Our recommendations are to engage these people and organizations:

WHO	WHY
GDPR Focused Cyber Security Experts	Experience is everything. You must engage consultants who have delivered successful Data Protection assessments and solutions. These consultants will understand the GDPR and appreciate what is required to meet the various elements.
Legal Specialists	If you have no internal legal team, you must engage with a legal entity au fait with Data Protection and the possible (as there are no test cases) repercussions of GDPR.
Vendors	No GDPR project will be possible, especially at scale, without deploying appropriate technologies; • Assessment • Remediation • Data Access • Auditing • Encryption • Workflow **not exhaustive*
Service Delivery / Service Integrator / SOC / Managed Service	An organization that can bring the above together. An organization that has not just the skills, but has the capability and resources available to deliver on time. An organization with the ability to provide program and project management to deal with internal and external stakeholders.

Some organizations will employ people to cover the above requirements, but most won't have the capacity or funds available to do so.

Contact your local STEALTHbits Technologies representative and they can put you in touch with recognized experts in each of the above categories.

At STEALTHbits we pride ourselves in being open and honest on where our solutions align against the GDPR articles and where we hand off to our comprehensive partner network.

The fourth blog in the series will discuss why STEALTHbits are a logical option for any GDPR project and run through the specific articles we address; ‘5 Essential Steps to GDPR Compliance. Part 4: Why STEALTHbits?’