STEALTHbits TECHNOLOGIES

CAS Severn

5 Essential Steps to EU GDPR Compliance: Part 5

GDPR—The Ticking Time Bomb

Source: The Insider Threat Security Blog

At the time of writing this blog, there are 378 days, 8 hours until the GDPR comes into force. That's 54 weeks or approximately 270 weekdays, not considering public holidays. Surely plenty of time to get everything in place and ensure your business is compliant. Right?

Wrong!

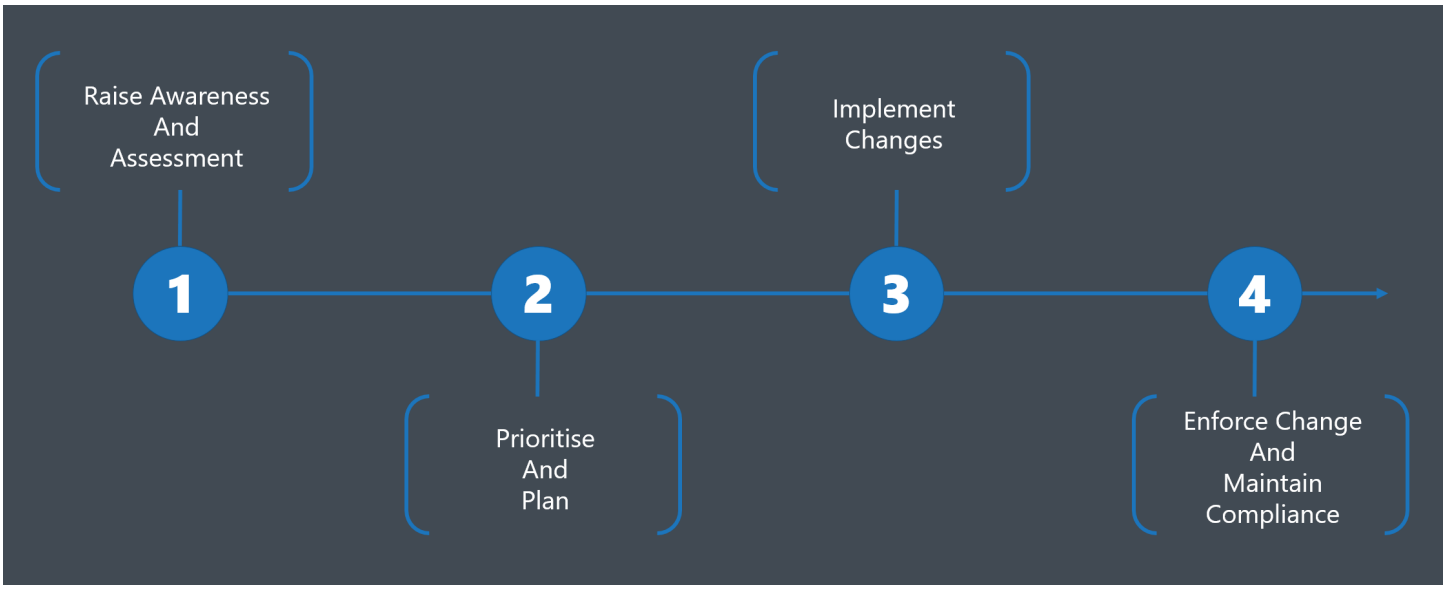
Let me back this up by putting some context around the various elements discussed in the previous blogs in this series.

The GDPR Project

Obviously, no two organizations are identical so for the sake of illustrating the point we are going to profile a run of the mill SMB organization and look at some of the critical undertakings required:

The Timeline

Something covered in Part 2 of this series. We can use the timeline as a guide and look at the task involved in each phase.



Engaging the right People

We also can't forget arguably the most critical requirement – engaging with the right people. Here's a reminder of who we recommend:

Internal	External
Information Technology	Cyber Security Specialist
InfoSEC	Legal
Human Resources	Technology Vendor (s)
Finance	Delivery Organization
Marketing	
Sales	
C-Level / Senior Management	

We aren't going to patronize you and outline how a project should be managed. We assume that you have all been involved in some capacity or other in a business wide project.

What we do ask is to remember the time, effort and challenges faced to get even the simple tasks completed.

Upfront Effort

- Getting stakeholders to buy in
- The business case (s) to get the buy in at C-Level
- Securing the funding for external resources. I'm sure you heard 'can we not do this ourselves?', more than once
- Going out to tender for the external bodies & vendors

The Project

- Putting together a project board/team
- Managing the team
- Change Control requirements
- Unknown challenges coming seemingly out of nowhere
- Coordinating and working to minimize disruption to business

None of this is unique to GDPR of course, but it should be a timely reminder of how tricky a project can be.

Now, let us add the nuances of GDPR…

The GDPR Effect

The Deadline

Where most project like to state a fixed deadline, that's often not strictly the case and frequently those deadlines slip.

There can't be any of that with GDPR. The deadline is May 25th 2018, period. No slippage. No light touch role out. May 25th GDPR is in force and fully in force. If you aren't convinced, here's a link to a session with the head of the ICO in the UK: https://iapp.org/news/a/icos-wood-gdpr-grace-period-no-way/

Change of Process

Very few organizations will have an end-to-end data handling process compliant with GDPR – and that's before you consider consent, DSARs and the right to be forgotten. Those efficient processes you have used for years may have to be completely revised. No small task.

Designing and testing the change. Implementing the change. Training the staff to work the change. Now there's a challenge!

DPO

You may have noticed the lack of DPO chat in these blogs. That's for good reason – it's not an area STEALTHbits can help you with. However, it's certainly one of the most critical elements if you come under the scope of requiring one. Do you need a DPO? Do you have someone suitable? What does a DPO do? They certainly won't be a cheap resource…even more expensive given the shortage of experienced security

personnel out there.

The Financials

We can't have a GDPR blog without mentioning the fines at least briefly. (for more information, please refer to part 1). The numbers are simply too large to ignore and ignorance is no excuse. However, it's not just the fine for non-compliance that you need to worry about.

Personal Litigation

If there is a data breach involving personal data, if you can't prove 'privacy by design and default', not only will you get hit with a GDPR fine but the Data Subject themselves will also have a case to take personal litigation action. These fines could dwarf and official fine and potential bankrupt an organization.

Share Value

Look at Amazon and the affect the well publicized breach had on their share value. GDPR related breaches and fines will be big news.

Add together these factors and non-compliance could bankrupt an organization.

Conclusion

We've taken a high-level look at GDPR, the well publicized elements and some that aren't immediately obvious.

We've highlighted who you should be working with and to what ends.

We've looked at the potential financial repercussions of not addressing GDPR – and soon.

I hope we have helped de-mystify some of the unknowns and given you clear direction and focus.

The EU GDPR is, without doubt, the future of Data Protection legislation, whether you are in the EU or not. Brexit or not.

Expect other territories to follow suit and tighten up their regulations.

Don't be a GDPR test case and headline.

Do call your STEALTHbits rep and we can help you on your path to GDPR compliance.