STEALTHbits TECHNOLOGIES

CAS Severn

5 Essential Steps to EU GDPR Compliance: Part 2

GDPR, The Data Access Governance Project

Source: The Insider Threat Security Blog

In part one we looked at the questions organizations must address when dealing with DSARs (Data Subject Access Request).

Simple questions, but in reality, tricky or virtually impossible to answer depending on the size and complexity of your data infrastructure.

That said, they're actually the core premise of Data and Access Governance.

What is Data Access Governance (DAG)?

DAG is best described as 'Governing who has access to what'. It's giving the right people access to the right data in a secure and efficient manner. When talking about DAG you will often hear the term 'POLP'. This stands for 'Principle Of Least Privilege' – everyone starts with access to nothing and is given access on a needs must basis.

These principles can be directly aligned to the key ethos of GDPR; Privacy By Design.

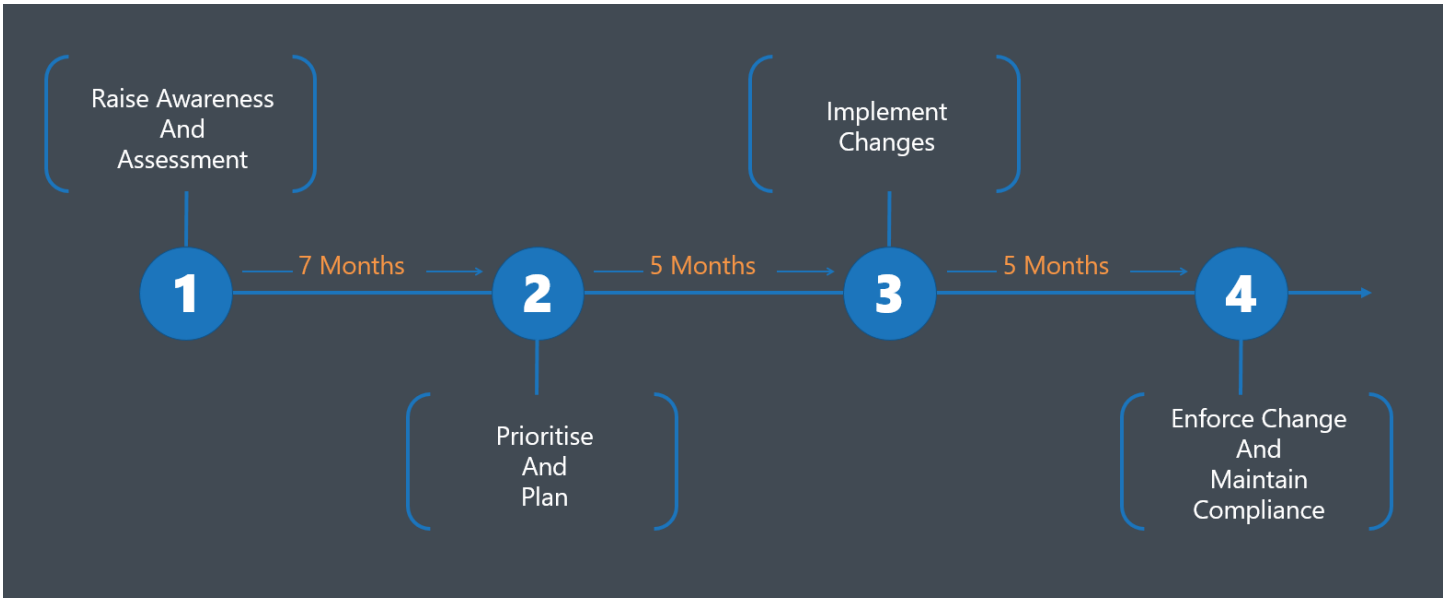
But what about the other elements?

As we get closer to D-Day (25th May 2018) more discussions are focusing on demonstrating the process and proving consent. Rightly so. These are critical to the process and should be equally top of your list of things to achieve, however, without the basics of securing and managing data none stand up.

It's important to understand the generic steps required to initiate your own DAG undertaking.

Once again, remove the 'GDPR' moniker for a moment and look at the timeline below, which is based on a

generic data transformation project:



Anyone who has been involved in a transformation project will be familiar with this project timeline. Why? Because these steps support any successful transformation and can't be skipped.

1. Raise Awareness

GDPR is not an IT or Infosec program. It impacts everyone in the business, from a call handler who takes information over the phone, through to Human Resources who will need to enforce the new policies. Don't let this be a surprise to the business on May 25th 2018

Assessment

You can do nothing without understanding what you have and where you are. Once you dig into your environment it's surprising the things uncovered.

I'm sure you've heard the cliché 'fail to prepare, prepare to fail'. Well, this is never more applicable than at the start of a data transformation project.

2. Prioritize and Plan

You can't do everything at once. An undertaking like this can and often goes on for months or even years. The priority for GDPR is around EU Citizen PII data, so prioritize it. To do that you must have completed stage 1.

Planning. Goes without saying.

3. Implement Changes

Obvious for sure. But how long will this activity take? It's not just the IT and technology to be implemented. Its business process and all the supporting elements around that. Don't under estimate how tricky this will be.

4. Enforce Change and Maintain Compliance

There's no point becoming compliant if you don't stay compliant. Sound obvious but is often not considered until it's too late. Maintain an oversite and understanding of your GDPR compliant data and processes.

On the diagram, you'll notice timings. These are an average for an average size organization. The key element is to recognize that a GDPR readiness project will be front heavy. Allow for that.

This sounds complex? Unfortunately, I can't say it isn't. It's also something that very few organizations can deal with internally.

This is why you should always look to engage the right people to help you comply and achieve it in time, which is the third blog in this series