Article

Aug 2021

Taming the (GDPR) Monster under the bed

The term 'GDPR' has become like that annoying hit record that stayed at number 1 for 13 weeks! We're all fed up of the constant inbox filling emails about GDPR seminars and meetings to the point where some of us may have pushed it way under our bed where it looms like a night monster waiting to attack on the 25th May 2018.

Beverley Robinson
Security & Compliance Manager
Email beverley.robinson@waterstons.com

Well, we're here to tell you that it doesn't need to be scary. Many elements of the new Data Protection regulation are actually the same as before and the new bits improve our rights and add some extra controls to ensure organisations handle our data how we would expect them to, without annoying us or putting our privacy at risk.

Firstly don't believe the 'buy this tool to be compliant', 'fines will be at the maximum', 'ICO will actively be trying to catch people out' headlines – that's just scaremongering. Instead, it's the simple things that will help you.

It's important to remember data protection affects us all. Just think about all the places you've had to share your personal details – name, address, telephone numbers and even bank details. Spend a moment writing a list of all the organisations that have some form of personal data about you. It's scarily big, isn't it! Now think about how you'd want those organisations to use your data. Putting yourself in the position of the 'data subject' will help you understand what your customers or clients may expect from you and help you to understand their concerns.

With this insight you're in a great position to tame that monster, by taking the following steps:

Understand the personal data you collect

How and why do you collect it? How do you use it and process it? What systems do you use and who do you need to share it with? This can be done by drawing out process flows (data mapping) from point of data collection to disposal, detailing all actions in between. (No you don't really need **that** automated discovery tool)

Define the legal purpose (reason) for collecting that personal data and the Legal basis

What are you relying on to be able to process the personal or special category data, such as legal requirement, contract, consent etc.? Top tip: choose consent only if others are not appropriate.

Consider your transparency

Be upfront about what you are going to do with the data you hold. Have you informed individuals clearly and simply what their data will be used for, how long it will be retained, who it will be shared with, what their rights are and how to raise concerns or exercise their rights?

Review your data maps and consider the security risks or non-compliance gaps such as:

- Have you got a **Data Protection policy and procedure** in place for how to manage rights requests, breaches etc.?
- Do you have a **privacy by design** approach, which includes building privacy concern mitigation in from the start and assessing risks using a Data Protection Impact Assessment (DPIA) process?
- Do you store data securely, only permitting access on a need to know basis?
- Do you **transmit data securely** via email or other sending and/or sharing outside your organisation using a private or encrypted link or an encrypted method?
- Have you set **retention periods** for all types of data in your organisation based on legal requirements or business needs?
- Have you **trained your people** to understand what Data Protection is, what their responsibilities are, how to appropriately handle, protect and secure data and what rights individuals have and how to handle them? Perhaps most importantly, where to get HELP!
- Can you locate, extract, delete, and preserve data if required to, in systems or otherwise, to ensure you could fulfil an individual's rights request?
- Are you **capturing consents** given and revoked appropriately, by channel (email, form, telephone ….), type of communication, recording individual data, time and method collected (verbal, email, online, written)?
- Are you paying particular attention to **special category** (health, race, ethnicity, sexual preference, trade union membership etc.), children's or criminal data?

Ensure you record everything

Yes, I do mean everything. Put all your preparations in one folder or a specific place, to ensure you can comply with the Accountability Principle which requires organisations to be able to demonstrate how they comply with the new Data Protection regulation.

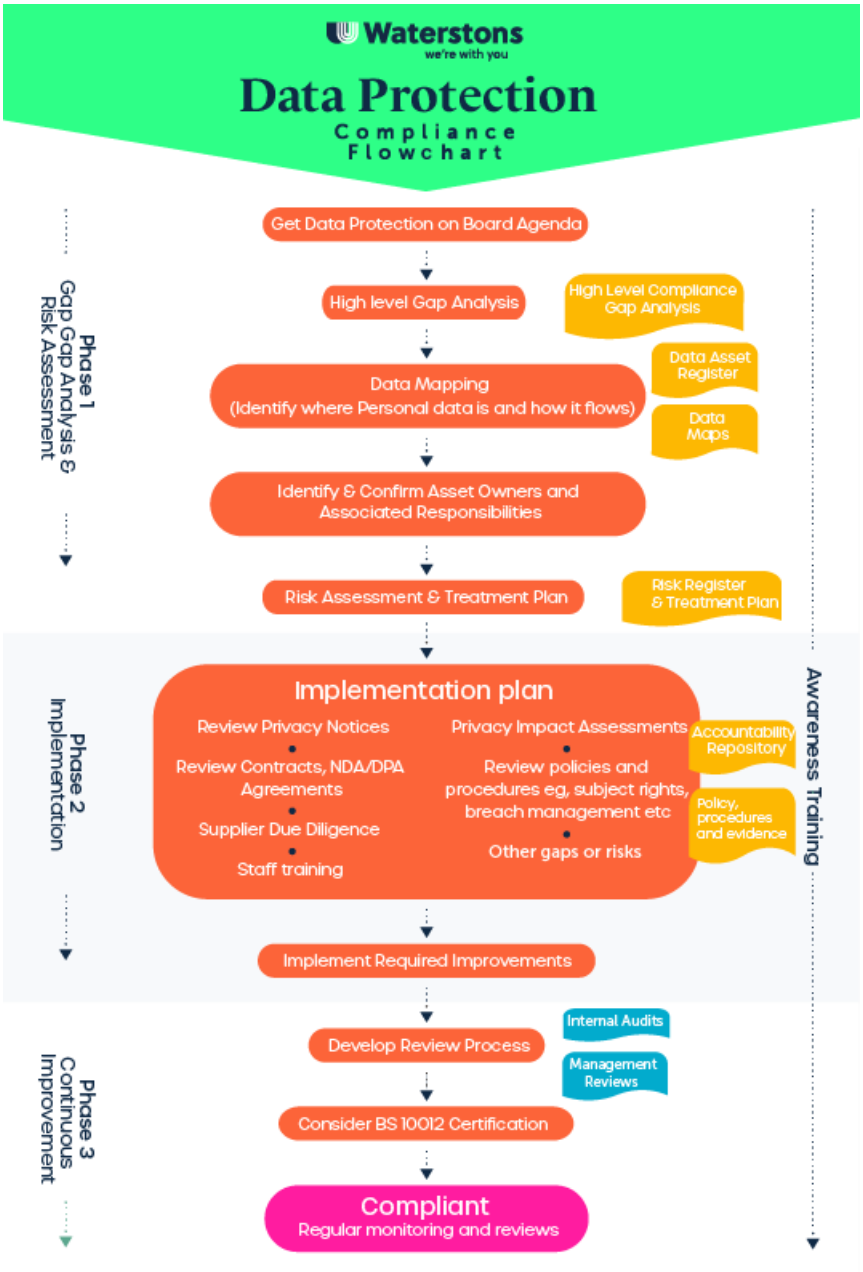
What happens if there is a breach?

If you have a breach the ICO will always ask you

- What policies and procedures do you have?
- How have you trained your people?
- How have you assessed privacy risks?
- How have you ensured you comply with the regulations?

Being prepared is your best defence to protect your organisation's reputation and future.

Our Cyber team have prepared a helpful flow chart below. If you need further assistance you can visit the ICO.org.uk website which has further helpful information and top tips, or you can contact our friendly monster slaying Cyber team!



Hopefully now you can sleep soundly with that monster tamed, or at least with a strategy and practical plan for dealing with it.

Sweet dreams!

PS - Our business monster slayers are also experienced in taming other business problems that may be keeping you awake. Why not give us a call?