COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2018
Stop debating and start acting: Apply GDPR in 10 steps

By Patrick O'Kane

Patrick O'Kane is Data Protection Officer for a US Fortune 500 Company in London, United Kingdom. He is the author of the book, GDPR - Fix it Fast.

- www.GDPRfixitfast.com
- linkedin.com/in/patrick-o-kane-cipp-e-cipm-cipt-3777928b

Like many people in the compliance sector, I often feel like I have reached the saturation point regarding the new European General Data Protection Regulation (GDPR).[1] Every day my inbox fills up with academic emails explaining some nuanced point of GDPR that is of no practical relevance.

The problem with GDPR is that it regulates an intangible: personal data. Therefore, it is a regulation that is hard to pin down. Too often the guidance we get from the "experts" tells us the "what" and not the "how" of GDPR. How do I apply it to my company, and what action should I be taking now?

My data story

I am a data protection officer (DPO) in London for a US Fortune 500 company. I have experience (in a previous DPO role) of running a large-scale GDPR project across 30 companies. Following are the 10 steps you can take today to breathe new life into your GDPR project. GDPR is an action regulation. The time for overanalysing has passed. Now it is time for action.

Step 1: Figure out whether you need to appoint a DPO

Under GDPR, you have to appoint a DPO if:

- You are a public body, or
- You carry out monitoring of individuals on a large scale, or
- Your "core activities" consist of large-scale processing of special categories of data.

It is important to remember that you will be in breach of GDPR and liable for the lower tier of fines if you do not appoint a DPO when you are supposed to. Article 83 of GDPR creates the potential for fines up to €10 million (about £8.7 million GBP or $12.3 million USD) or 2% global annual turnover for breaching the rules on DPOs.

Step 2: Carrying out a data audit

It has been said that more data is created every two days than was created from the dawn of civilization until 2003. Your company has likely been amassing large quantities of data. To get in line for GDPR, you first need to figure out where your data is.

To start your data audit, you should:

- **Prepare a questionnaire**: You should prepare a questionnaire that asks for details on how data is processed.
- **Send it out**: Send it to all departments of the company.
- **Follow up with meetings:** You should follow up to get a better understanding of how it is processed.

Step 3: Draw a data map

To help you understand where the main risks are on GDPR, you will need to draw up a map of where your data is, who it is shared with, and where it is being sent. You can use the map to help you figure out your main GDPR-related exposures.

In brief:

- **Map the data flows**: Drawing a map of the data flows helps pinpoint the issues.
- **Prepare a risk register**: You should prepare a risk register that outlines:
    - the major risks in the way data is being used,
    - how these activities could breach GDPR, and
    - what you need to do next.

Step 4: Get straight on security

I probably shouldn't be saying that one step is more important than the others, but I can't stop myself. Data security is likely the most important part of your GDPR project. Get this right, and your project is in a strong position. Fail on data security, and your company could be in line for some major GDPR fines.

My top tips are:

- Inspect your company to see where the data security holes are;
- Train your staff on data security (see Step 7 below);
- Make sure you have adequate cybersecurity, including breach prevention, software patches, penetration testing, and encryption; and
- Put a data breach response plan in place.

Step 5: Stop using painful privacy notices

Can you remember the last time you read a privacy notice? Me neither. Even in the privacy business, we are still not reading privacy notices. GDPR expects more. We are to engage our customers and make our notices clear, plain, and concise.

My tips:

- Keep it as short as possible and use short sentences
- Avoid jargon

- Set the privacy notice out in a clear way with a good structure, and
- Keep the tone helpful and friendly

Step 6: Sorting out your company policies

A big part of GDPR is being able to "demonstrate compliance" (Article 5) (i.e., to show you are complying with the new regulation in all that you do with personal data). To do that, you are going to need to make sure you have the appropriate staff policies in place that can educate your workforce on their responsibilities regarding data processing across your operations.

You may need some new policies, such as a data breach incident plan, big data policy, Human Resources data protection policy, marketing and data protection policy, social media policy, and bring your own device policy. Figure out where your policy gaps are and fill them.

Step 7: Staff training

Companies often underestimate the importance of staff training. One recent study found that human error is a leading cause of data breaches, featuring in 37% of data breaches.[2]

My top tips for training staff are:

- Deliver basic data protection training to all staff.
- Work out who needs face-to-face training. Is it Marketing, Legal, etc.?
- Make it engaging and relevant with lots of examples of how it affects their everyday life and their job.
- Record all training you carry out. It will be useful if a regulator ever comes knocking.

Step 8: Draft a template for privacy impact risk assessments

Under Article 35 of GDPR, we have to complete a data protection impact assessment (DPIA) for higher risk data projects. A DPIA is a form that must be used on new projects if you are using "new technologies" and the processing is likely to result in a high risk to the rights and freedoms of individuals. You need to put a process in place to ensure these DPIA forms are used, because failure to use them can attract heavy fines under GDPR.

Step 9: Reporting data breaches

Under Article 33 of GDPR, there are rules related to notifying regulators of some data breaches within 72 hours. Under Article 34, there are also new rules related to notifying the individuals affected by data breaches without undue delay.

Failing to report these breaches where the regulation requires it, or failing to report them in time, can attract major fines. Two major tips:

- Educate your employees on their new responsibilities to report data breaches.
- Have a process in place so that breaches can be reported to regulators and customers efficiently.

Step 10: Dealing with contracts

Under GDPR, when we use a vendor and we entrust them with our data, we must, by law, have certain clauses in the contracts with that vendor to ensure that they keep our data safe. This applies when we are a data controller hiring a data processor to do work on our behalf. It also applies when we are a data processor hiring a sub-processor.

My top tips are:

- Make sure, going forward, that your contracts with suppliers and vendors have in place all the GDPR clauses set out in Article 28.
- Decide which of your historic contracts need to be updated.

Remember that GDPR is an action regulation, so get to work today on closing your GDPR gap.