ProvePrivacy

First 100 days of a data protection project; planning for success.

www.proveprivacy.com
hello@proveprivacy.com

As a data protection professional, ProvePrivacy Founder Mark Roebuck often gets asked what the most important aspects of data protection are. Whilst there are many things in the regulation that tend to resonate and help shape advice to clients, it is difficult to list which are most important as the answer is reliant on the context.

In this guide we share Mark's recommendations and insights on what the first 100 days of an engagement should include, outlining what should be planned for, whilst allowing room for change in line with circumstances.

Understand your activities

What activities does your organisation undertake? Without knowing how your organisation uses personal data you cannot begin to understand any data protection risks. Even if you don't fall under the mandatory requirement to create and maintain a 'record of processing activities' (RoPA), it is a good tool to use to evidence how you process personal data.

Understanding your activities means,

- Understand what you do
- Knowing the personal data which is processed
- Understanding the volume of data
- Understand the type(s) of data used

These are the key aspects to begin understanding the potential for high risks.

1. Determine if data subjects know how you are processing their data and what lawful basis you are relying upon to undertake each activity. This can be particularly important where personal data is received from a third party. A Fair Processing Notice on your website is no good unless data subjects know that you are processing their data in the first place.

2. Understand where your data is stored, information assets such as forms and systems need to be treated in different ways. Knowing where data is stored helps understand any third parties being used to store it. Information collected at this point will also useful to IT departments, and help build relationships with them.

3. Identify your third party data sharing relationships. This will help you understand any contract risk as well as international data transfer assessments which might need to be completed. If an activity has been assessed as high risk, you may want to consider undertaking a security assessment on related third parties.

TIP Mark recommends that a brief assessment against 'high risk criteria' is undertaken for every activity. A short assessment takes very little time and will allow you to evidence that you have considered the risk.

TIP Mark suggests that when creating and reviewing the RoPA, that you involve the stakeholders responsible for the activities. The more involved they are in the process, the more they take ownership of the risks.

Manage the risks

Whilst a RoPA is not a regulatory requirement for all organisations it provides valuable insight into organisations.

Involve others in the management of risk. If a risk is identified on a HR activity, let HR lead on the solution, especially as it is their procedures that will need to be amended. Risks can remain unchecked if there is poor ownership and low accountability, regular meetings to review progress and provide advice are a must.

Good risk management starts with identification and continues with good planning. Ensure that an action plan is defined to mitigate the risk and monitor that the plan is being delivered. It may not be possible to mitigate a risk entirely, so ensure that if any residual risk remains it is understood and accepted by the accountable stakeholders.

Don't forget that there are at least two impacted stakeholders when managing risk. The data subject and the organisation. An ideal risk plan will mitigate the risk to both, but this might not always be possible or practical. You can allow others in the organisation to accept a residual risk to the organisation, but you should consider 'proportionality' when considering any risk placed upon the data subject.

The job of a data protection professional is not to eliminate risk, it is to manage it and accept that sometimes others will need to live with a risk, when this is the case ensure that a record of that decisions is kept.

TIP Mark suggests considering your findings from data breach and data subjects rights logs. These will help you to identify recurring incidents, which in turn identify risk. Record these risks and manage them.

Teaching and Learning

Understanding the risks allows individuals to learn how to mitigate them and put plans in place to stop them from recurring.

Clear policies and procedures need to be developed and communicated, these should be supported by good data protection training. People cannot be expected to protect personal data and keep it secure if they don't understand how data protection rules apply.

Employees should complete training in the basics of data protection as a minimum, and feel empowered to make reasoned decisions.

The knowledge individuals need will vary depending on their role. Managers, leaders and those who are involved in defining a RoPA should be well informed and able to lead by example, identifying any gaps in their team's knowledge.

ProvePrivacy recommended the following as a minimum:

- Information security training covering the dangers of phishing, hacking etc. Ensuring that colleagues understand key principles for protecting data when in the office, on the move or working from home.
- Understanding of what a data breach looks like, the most common causes and what to do if they suspect one has happened.
- Understand privacy rights such as the right of access, right to object and right to erasure and what to do if they receive a request.
- Knowing the way they are processing data is fair and lawful.
- Understanding the guidance for secure storage and sharing of personal data.

RECOMMENDATION Mark recommends annual online data protection training supported by regular engagement and short reminders throughout the year. Making training part of routine develops an automated response in colleagues when they spot an event.

Try to create easy to understand policies and guides. Consider if short videos work for regular issues, such as data breach awareness. With more than three quarters of reported breaches the result of human error training and understanding really is crucial.

Use real events to support your training, whilst data breaches and subject rights requests are a valuable source for risk, they also allow us to learn. When something happens, communicate it in a fair and anonymous way so that colleagues are encouraged and learn from real life examples.

Data Protection by Design and by Default

By building engagement through the development of the RoPA colleagues will begin to understand that data protection risks can be resolved through good practice and procedure. As such a new project being initiated or a procedure being changed is a great opportunity to consider if data protection can be built in at the point of design.

Relationships with project governance teams are crucial, if your organisation has a project function, get to know your Project Management Office (PMO) and ensure that data protection questions are built in at different project stages. If your organisation uses an agile approach, get to know your Product Owners and ensure they involve you in planning and retrospectives.

TOP TIP Mark believes that good organisational design is key to ensuring that any process works effectively, not just data protection. Consider setting up a Data Protection Working Group, involve your RoPA stakeholders and develop a regular cadence that suits your organisation.

Accountability

One of the key differences between the Data Protection Acts of 2018 and 1998 is the principle of accountability, ensure your first 100 days is focussed on this.

Accountability means many things including:

Senior engagement

Are you engaged with senior levels of management and are they supporting you? A report to the Executive team on a monthly basis should be a minimum goal. This will allow concerns to be expressed, risk acceptance achieved and support for the work gained.

Maintain records

Accountability is about evidencing compliance with data protection laws. Many of these have been covered, including policy, procedure, RoPA, risk logs and actions as well as incident management.

Data Champions

Although they may not be called this in your organisation these individuals are the established network across functions who take accountability for data protection in their department. Meeting regularly with this group will help foster responsibility at a functional level.

Maintaining accountability is now one of the pivotal requirements of the data protection act but it is not the responsibility of the DPO alone.
This makes training and awareness at all levels key.

Summary

- Focus the first 100 days in your role on learning and coaching. You need to learn what risks your organisation has and teach stakeholders how to manage current risk and reduce future risks.
- Building relationships is key, formalise these through regular meetings where data protection is the focus and you will begin to develop a culture which supports your role in the organisation.
- Manage upwards as well as amongst your colleagues. Not all Executives will take data protection seriously from the start so build close connections with those that do and that will support you.
- Ensure that you have systems in place to evidence compliance that works for the size and scale of your organisation.