GDPR

Coming to an information commissioner near you – May 2018!

So why should I comply?

If you process personally identifiable information (PII) in the UK, then you should already be complying with UK legislation – Data Protection Act 2008. The General Data Protection Regulation (GDPR) just tightens up data control and processing for all EU citizens whether you are in the EEA or not. So if you control or process any EU citizen's data then you will have to meet these regulations, no matter which country your business is in!

Additionally, the GDPR also has teeth. Whereas the UK Information Commissioner could currently fine a company up to £500k, if you make a disclosure. The GDPR requires mandatory notification on breach and penalties for a breach could be up to 4% of global turnover or €20 million – whichever is larger. Custodial sentences will also still be possible for data protection breaches under other UK legislation.

Background

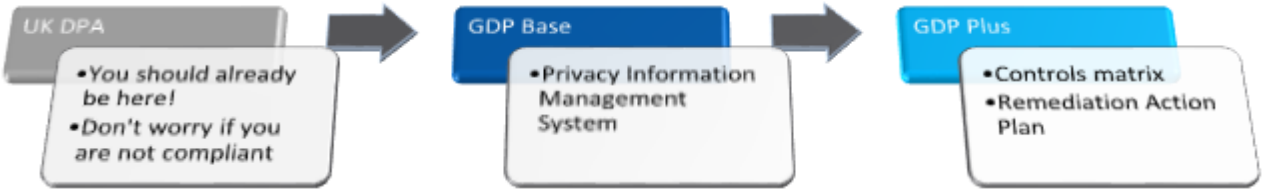
There is limited information and guidance that is available today on the implementation of changes between the UK data protection act and the General Data Protection Regulation (2016/679). The ICO in the UK has published limited information at the current time and this identifies the areas of change and what you need to think about.

If you process data from any EU citizen, then you will have to comply with the GDPR. Now that Article 50 has been triggered, it will take at least two years to exit, so the regulations will have been passed in the UK parliament and will be in force. As such this regulation is coming and you need to consider the implications to your business.

As with all regulations these are written into law without full consideration of the size of the organisation, the complexity or the practical application of how you as a business will implement, monitor or maintain compliance. There is no overarching standard like you have in the payment card industry (with the PCI DSS), or defined auditable process. As such you usually have to come to the conclusion yourself about what the right and best thing to do is.

How can we help?

If you are a Small to Medium Business (SMB) then our services are designed to clear up this confusion for you. If you are an enterprise customer, then see our guide on our GDP Enhanced service. As we see it, there are two aspects that you need to consider in relation to successfully securing privacy information. These are the management system you use to govern the data and the controls that you put in place to ensure the Confidentiality, Integrity and Availability of that data. Therefore, we designed the GDP base service and the GDP Plus service. These build on top of each other and are complementary to both the UK Data Protection Act and each other:

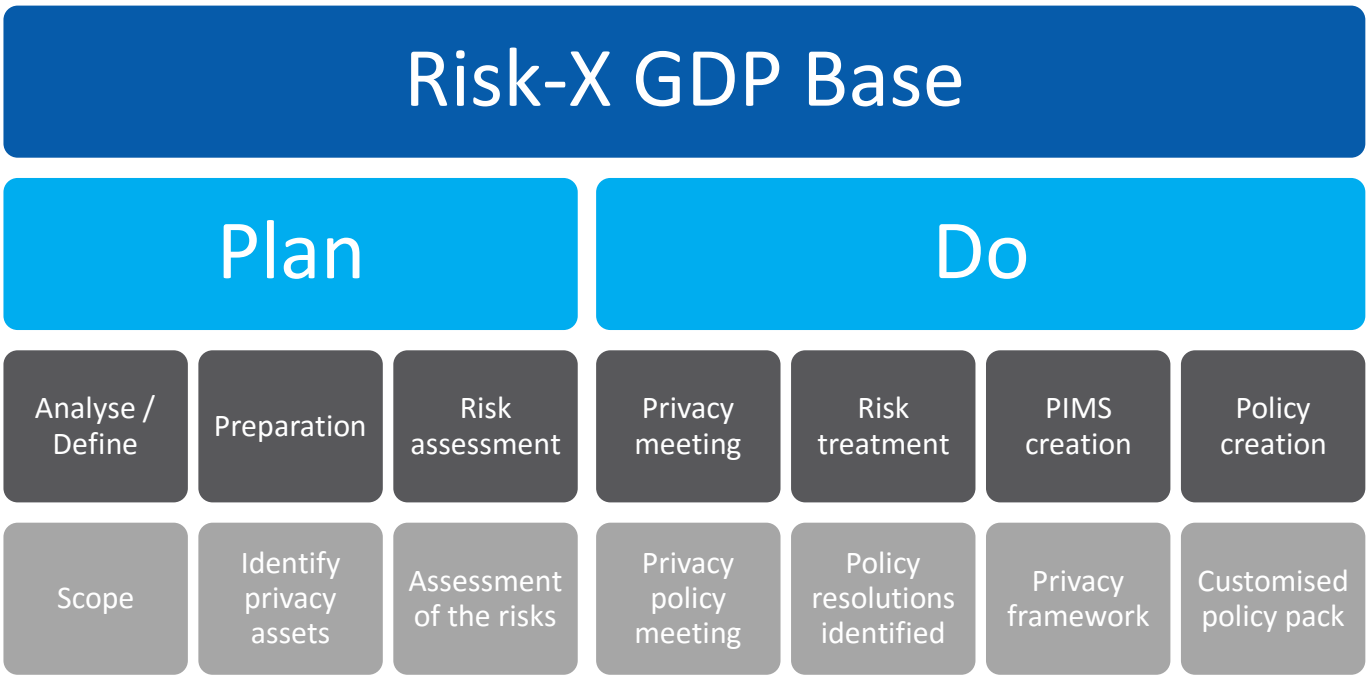


The following datasheet information builds on these requirements for the SMB customer, so keep reading!

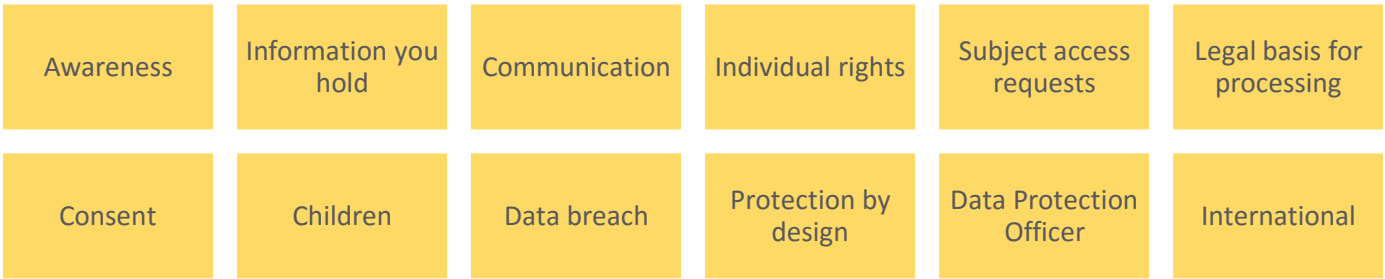
General Data Protection Base

The base level service has two main goals in mind. Understanding your business and providing you with the paperwork that you will require. Before you can undertake any form of control around the privacy information you have, you need to know where it is, what you use it for and by whom. For most companies they have some idea, but generally this is a challenge for customer data, let alone internal information. This is complicated if you have your own customer data or data from other companies on behalf of their customers.

Risk-X have designed the GDP base service in line with the most well recognised international standard for the security of information – ISO27001. The premise of the GDP base product is to help you identify what information you have and how you use it. Once you understand this then a Privacy Information Management System (PIMS) and appropriate policies can be created to manage this data. The process that we use to do this is as follows:



When you complete this exercise you will have a workable Privacy Information Management System (PIMS) and will be able to address the 12 key points that the UK Information Commissioner's Office (ICO) has recommended that UK businesses should focus on to ensure that they can meet the new regulation. These areas are:



This service focuses on the basics of data protection to ensure that you can get these right. This exercise is consultant led so that you have the ability to interact and ask questions. The goal is to leave you with a working system and all of the policies that you require to comply with the recommendations in line with the regulations. These documents will become working documents inside your organisation that can be updated as things change.

Once you have your management system in place, then it is time to look at controls, see our GDP+ solution.

General Data Protection Plus (GDP+)

The add on to the GDPR Base service comes with the plus bundle. This takes the work you have already completed and extends this to the operational, physical, technical areas of your business and considers their implemented state. Our consultants will look at the scope that was generated with the Base service and then use ISO27001 (aligned with privacy frameworks) to review how your data is protected. The report will focus on two areas:

The first being the statement of applicability of controls. This grades whether the control is required for the security of privacy information, and then tells you whether this is in place or not. This area of the report will look as follows:

A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	**Applicable**	Not in Place	There is no formalised information classification policy - currently common sense is heavily relied upon
A10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	**Applicable**	Partial	Some controls are in place but there is a limitation of the areas which are covered. Internal machines protect against malicious code, but public facing web servers do not. Additionally, there is no process for users to report issues to their helpdesk if a virus is found

The second being any areas that are non-conformant to ISO27001 will be added to a remediation action plan. This will be risk prioritised within your organisation so that you can see which areas need to be changed first, a summary is shown below:

Risk	Issue	Resolution
	DPA information and controls Privacy information is not subject to good security controls in certain instances, and these include: • DPA data sent in spreadsheets and only password protected • Marketing copy PII data onto laptops • Access to information is available if this is stored in the incorrect locations • Email used to send data • Shared drives exist with copies of marketing data including PII	Data classification guidelines were produced during the GDP lite engagement. These should be applied to all of the identified data within your systems that has been identified. Users need to be educated on what is required and how data should be used and secured. Data should always be retained inside the environment and regulated data should not be removed.
	No Anti-virus / Anti-malware (AV/AM) on web servers In general, the operating system (X) used is secure. However, the applications installed on (X) allow for significant attacks to occur against these systems. Coupled with limited testing and security deployment at this layer it can be trivial to compromise these web services due to the applications or poor coding practice. AV/AM will not prevent this, however it can be used to prevent the standard exploits that the hacker will then run. In our experience over 60% of our forensic cases would not have been investigated had this been in place.	As part of a defence in depth strategy Company X should consider: • Implementation of AV/AM on sensitive machines within the environment (this should include web, application and any server that is open to the internet) • That this should allow for real-time scanning as well as scheduled • That this should be regularly updated, both programme and definitions • That logging should be kept for one year and centralised to prevent tampering

The GDP+ process looks at all areas of the business in scope for privacy information and provides a baseline of all of the controls that are in place. Further guidance is then provided to allow you to remediate any areas of failure. ISO27001 is a great standard to use for this process and lends itself directly to privacy requirements. You may decide to then uplift this to cover all areas of your business. The great thing about this service is that the GDP+ process does not have to directly follow the GDP Base service, it is recommended, but can always be bolted on later.

ADDITIONAL SERVICES

Don't worry if you need more help or are an enterprise customer, we can provide additional services you may need:

Data discovery	Subject access request tooling	Training	Data protection officer	Legal support	Assurance testing	Incident response	Forensic investigation

Why Risk-X?

Risk-X has been working on data security with clients who process personal data across many industries for a long time. The traditional methods of handling, processing, transmission, storage and sharing are not adequate for the new regulations. Our work with payment card data, one attribute of personal data, has taught us that a new approach is required. With the changes the GDPR will bring, Risk-X is best placed to help you: find, search, collate, rationalise, optimise, streamline and ultimately comply with the requirements prior to the deadline of May 2018. This is due to Risk-X having all of the elements you require from Audit & Advisory, Forensics & Incident Response, Legal, Training and Assurance testing. Why not call one of our key contacts to find out how we can help.

Key contacts

Steve Marshall
Senior Partner / Exec Chairman
Steve.marshall@risk-x.co.uk
+44 7770 352438

Kevin House
Partner / Director
Kevin.house@risk-x.co.uk
+44 7580 834803

John Cranmer
Senior Partner / Director
John.cranmer@risk-x.co.uk
+44 7974 445505

Andrew Gilhooley
Partner / Director
Andrew.gilhooley@risk-x.co.uk
+44 7580 834586

Qualifications

ISO27001 Lead Implementer
Our consultants hold the ISO27001 lead implementer qualification

ISO27001 Lead Auditor
Our consultants hold the ISO27001 lead auditor qualification

PCI DSS Accredited
Risk-X LLP (formally Pentest Partners Consulting LLP) are a PCI QSA company

PCI PFI Accredited
Risk-X LLP (formally Pentest Partners Consulting LLP) is a PCI Forensic Investigator (PFI)

CISM
Some consultants hold the Certified Information Security Manager certification.

CISA
Some consultants hold the Certified Information Security Auditor certification

CRISC
Some consultants are certified in Risk and Information Systems Control

CISSP
Many Risk-X consultants hold the CISSP certification.