Grant Thornton

An instinct for growth™

Data Protection

Spotlight on the new data protection laws

Data protection law is evolving. The introduction of the EU General Data Protection Regulation (GDPR) has prompted the introduction of revised local laws within the Channel Islands, in order that the Islands' laws remain in line with those of the EU. Although data protection legislation has been with us for over 20 years, much has changed in that time: the new regulations reflect this.

Most organisations that work with Personally Identifiable Information (PII) are subject to data protection law. PII encompasses everything that could be used to identify an individual – names, addresses, phone numbers, email addresses, passport numbers, … the list goes on.

The laws are not inherently complicated – they are written in reasonably comprehensible English – but they are lengthy and contain a huge amount of rules with which organisations must comply. There are various penalties for failure to comply, including not just fines but also other sanctions such as being instructed to cease processing some or all data sets until the breach has been rectified.

This guide provides a starting point – the top ten aspects of the new data protection laws that you should focus on first. Each point provides pointers to some of the key sections/articles of the laws in question; these are not designed to be exhaustive, but to point you to a handful of the most relevant sections.

Links to the PDF laws are provided at the bottom of the page.

1 Understand your data

If you're to conform to the law, you need to know what PII you're working with, what you're using it for, and where it's stored. You also need to understand the sensitivity of the data, since the laws consider some types of data (for example health data or information about race or sexual orientation) to be more sensitive than others and demand more stringent controls over those elements. You also need to be confident that you're holding each data item for a good reason.

For example, if you run a small construction business, common sense dictates that you need customer name and address data for billing purposes, but you probably don't need to know (say) their religion or country of birth.

And don't forget that paper copies of PII are just as relevant as electronic copies in the eyes of the law.

Jersey DP Law: 9	**Jersey DP Authority Law:**
Guernsey DP Law: 6	**GDPR: 6**

2 Data retention and destruction

As well as knowing the data you hold, you must be conscious of how long you need to retain it – and you must delete it when it is no longer reasonable to hold it. You must have a data retention policy, which lists the various data types and locations and states the retention period, and you must follow this policy – delete data when the policy says you must. It's human nature to hold on to data "just in case", but the law prohibits this.

In some cases the retention period may be dictated by the law or a regulator (e.g. the retention of bank and tax records for a statutory period). In cases where the retention period is not mandated, you must consider what is reasonable: for example you may decide to delete customer names and addresses if you have not dealt with a customer for 12 months. And if the person to whom a data item relates requests that you delete it, and their request is reasonable, you must do so.

Jersey DP Law: 31, 32	**Jersey DP Authority Law:**
Guernsey DP Law: 7, 20, 21	**GDPR: 16-17**

3 Data Protection Officer (DPO)

Many organisations are required by the law to nominate a DPO. Examples are public authorities, or private companies doing large scale processing or working with sensitive data. The DPO must be someone with a good understanding of the field of data protection, and must have capacity within their schedule to do the job properly (i.e. it's not permitted to nominate someone in name alone just so you can claim to have a DPO). If your organisation is a group of companies it's reasonable to have a single DPO spanning more than one entity, so long as the workload is within their capacity and it is logistically reasonable for them to work with those entities.

It should be noted that staff education, as described in item *6: Training and awareness*, is the responsibility of the DPO where the organisation has one.

Jersey DP Law: 24-26	**Jersey DP Authority Law:**
Guernsey DP Law: 47-51	**GDPR: 37-39**

4 Secure Systems

It is essential that you take care to store your data securely, so that it can't be overseen, stolen or copied by an unauthorised party. Printed documents should be stored securely in locked cabinets, rooms and/or buildings.

Computer systems should be protected against attack by installing anti-malware software, by ensuring that unwanted users are unable to connect to or log into systems, and by having firewalls protecting you from the Internet. The Cyber Essentials accreditation (https://www.cyberessentials.ncsc.gov.uk/) is the recommended minimum standard for IT systems. And if you take PII off-site, for example on a USB memory stick or hard disk, be sure to encrypt it and preferably use a device that has its own built-in encryption features.

Jersey DP Law: 8, 21	**Jersey DP Authority Law:**
Guernsey DP Law: 6, 41	**GDPR: 5**

5 Breach reporting

A "breach" is any unlawful or accidental incident that causes PII to be: disclosed to an unauthorised party (e.g. by a computer system being hacked and data accessed); deleted (by a hacker erasing the contents of a file, for example); or corrupted (e.g. by a ransomware attack encrypting files irretrievably).

A breach must be reported to the Data Protection authority – even if you only suspect it has happened and have yet to confirm this – within 72 hours of it being discovered or reported to you. Depending on the nature of the breach you may also have to inform other parties, such as the individuals to whom the data relates. Prompt, proactive reporting is always better than being reported to the authorities by a third party.

Jersey DP Law: 20	**Jersey DP Authority Law:**
Guernsey DP Law: 42, 43	**GDPR: 33-34**

6 Training and awareness

As with any law, ignorance is not an acceptable defence in the event of a data breach. It is essential, therefore, that all the people in your organisation have a basic understanding of the requirements of data protection and how they should go about their day-to-day duties when working with PII. This training should tie in with the controls you have in place as per item *9: Security policies and procedures*. Such training is the responsibility of the Data Protection Officer (see *3: Data Protection Officer*) where the organisation has one; in other organisations a suitable individual or group should oversee and manage the training regime.

Jersey DP Law: 26	**Jersey DP Authority Law:**
Guernsey DP Law: 50	**GDPR: 39**

7 Supply chain

Organisations seldom operate in isolation: it is therefore common to exchange data – including PII – with third parties such as suppliers and customers. Make sure that staff are cautious when sending information to customers: inadvertent slip-ups can cause data to go to the wrong place. And if you engage a supplier to carry out work that involves PII you are sending to them, be sure that the contract between them and you makes clear the nature of processing to be done and their obligation to protect it adequately. Even if you engage a supplier to process data on your behalf, the buck stops with you in the event of a contravention of the law.

Jersey DP Law: 7, 19, 23	**Jersey DP Authority Law:**
Guernsey DP Law: 33-36	**GDPR: 28-29**

8 Registration

If you are working with PII you must register your activities with the Data Protection Authority, and failing to do so is an offence. Registration involves describing the type(s) of data you will be processing and the way(s) in which you will be processing the data, so prior to registration you need a thorough understanding of the PII you are working with.

The registration process is straightforward, and the Data Protection authorities' Web sites have plenty of helpful guidance notes.

Jersey DP Law: 24	**Jersey DP Authority Law: 17**
Guernsey DP Law: 39	**GDPR: 37**

9 Security policies and procedures

Compliance with data protection laws is made easier by having strong controls over the way staff work with PII. You should therefore define standard ways of working with systems and data and ensure that the people in the organisation conform to them. Examples are to prohibit the sharing of passwords for computer systems, or to instruct staff not to send sensitive information via unencrypted email.

Once you have your collection of policies and procedures you need to instruct staff in their use as discussed in item *6: Training and awareness*.

Jersey DP Law: 8, 21	**Jersey DP Authority Law:**
Guernsey DP Law: 6, 41	**GDPR: 5**

10 Subject Access Requests (SARs)

Anyone whose PII you work with has the right to request a copy of the data you hold on them. You must provide that information free of charge, and unless the request is particularly complex you must do so within a time limit (four weeks in Jersey, a month in Guernsey).

Be sure to react quickly to such requests, particularly if your systems are such that it can take some time to extract the requested information.

Before sending the response to an SAR, make sure you are confident of the requester's identity and that it is lawful for you to send the data to them.

Jersey DP Law: 27-28	**Jersey DP Authority Law:**
Guernsey DP Law: 15	**GDPR: 15**

Useful links

Data Protection Authorities:

- **Jersey:** https://dataci.je/
- **Guernsey:** https://dataci.gg/

Links to legislation:

- **Jersey Data Protection Law (draft)** http://www.statesassembly.gov.je/assemblypropositions/2017/p.116-2017.pdf
- **Jersey Data Protection Authority Law (draft)** http://www.statesassembly.gov.je/assemblypropositions/2017/p.117-2017.pdf
- **Guernsey Law** https://www.gov.gg/CHttpHandler.ashx?id=110559&p=0
- **GDPR** http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

grantthorntonci.com