Data Protection – Frequently asked questions

What is it and why is it here?

How long has data protection been in place in Jersey?

Data protections has been in Jersey since 1987, however it was in 1995 that the landscape properly changed and the first set of legislation was introduced.

Why is data protection legislation being changed?

The landscape of our lives has changed dramatically over the past 30 years such that technology and data is much more sophisticated and prolific. Social media and the many devices that people use on a daily basis are leaving a digital footprint about our lives. The volume and type of data this is now being created needs to be much better regulated so that the people who use, collect and access this data use it properly and for the right reasons ensuring that you as a citizen are better protected.

Who needs to register with the information commissioner?

Any business that collect, handles and stores personal information must register with the information commissioner regardless of its size, however, if you are a freelancer, very small business or charity you'll pay a different fee from larger organisations, and in some cases, no fee at all.

Data processor vs data controller

- A data controller is an organisation not an individual. Whoever heads up the organisation has ultimate responsibility but everyone in the business who has

access to the data needs to understand the obligations of a controller.

- A data processor is an organisation that processes data on behalf of another. For example, you might outsource tasks to others who run operations on your behalf and they, such as your accountant, cloud service provider, payroll manager are processors. Data processors are suppliers to you and so you need to have a processor agreement in place to make sure they are doing the right thing with your data and not mishandling it.

Who does it apply to?

I'm a sole trader, does Data Protection apply to me?

It is more important to think about the type of information that you are holding rather than how big you are as an organisation. Consider how sensitive the data is, what you do with it and what you need to do to keep it secure. Adopt a sensible approach to making sure that you are handling the data properly and sometimes it's the simple things, such as putting password protection on individual documents that work best.

Does Data Protection apply just to me as a business owner or to everyone in my organisation?

Your business, as a data controller, is responsible for the personal data it holds so all your employees need to understand what the business expects of them in terms of using and sharing data, however, as the owner of the business you are ultimately responsible. Employee training is a vital part of making sure all your staff know what their obligations are & don't share information unwisely. Historically staff are the biggest risk area when it comes to data breaches so this is worth spending time on and perhaps having written policies in a staff handbook.

I'm collecting personal data because I have to comply with AML or KYC regulations, are there any special rules for this?

If you have a legal requirement to collect specific information about individuals then you are collecting this

because of a ‘legal obligation’ and so additional consent is not necessary.

However, to be fully transparent you are still required to make sure the individual is fully informed about your data processing activities and so it’s necessary to have a privacy policy which you share that explains the information that you are holding and why.

Handling personal and client data

I don’t understand the difference between the ways I am legally allowed to process personal data

You can only process a person’s data if:

- the individual has explicitly allowed you to process their personal data for a specific purpose (**Consent)**.
- you need to process the data for the performance of a contract between you and the data subject (like an employment contract or service contract) (**Contract**);
- you need to protect someone’s life (**Vital Interests**).
- it’s in the public interest or for your official functions, and you’ve got a legal basis (**Public Functions**)
- it’s necessary for your legitimate interests or the legitimate interests of a third party (**Legitimate Interests**).

What do I need to tell clients about how I am using their data?

You need to let clients know certain things when you start to use their data such as who you are, what data you are holding and what you will do with it. Part of this requirement is how long you will keep the data for which should be the length of time you realistically need to keep it or are legally obliged to keep it.

Think about creating a consent or information form when you start working with a client which might collect data but also indicate how you are going to use the data to provide the product or service. Use this to explain what you’ll have to do to provide the product or service so you don’t need to have a consent for every single element of

that service. For example, if a client has been referred to you from their doctor for treatment, you might say that you'll send a report back to the doctor about your proposed treatment. However, if you then want to use their data to do something completely different – like marketing to them – then it would be good to have a tick box to get their consent for that type of communication. Remember that if you do this, you cannot pre-tick the box as the customer needs to 'opt-in'.

Are there rules about how long I can keep client data for?

When you think about how long you are holding data for think about what's reasonable, for example, if it's a one off activity or job then you'll need it for a shorter time then you would need to keep data for a long term project or an ongoing client relationship. You may also have a legal obligation to hold information for a particular length of time, for example KYC information if you are a regulated or financial services business. It's a good idea to have a very basic document retention process which you go over on a regular basis.

My staff use ID cards with personal information that can be accessed by clients, who is responsible for the data on these cards?

Technically the information on the card belongs to your business as the data controller but you can pass on some responsibility to the individuals to ensure they use the card responsibly. In addition, you should ensure that the customers that are accessing that data have appropriate measures in place to ensure they are holding and managing the data in accordance with data protection requirements.

Sharing data with third parties

We give warranties for our products and share personal data with the warranty providers, is this a problem?

When you are selling your product you need to be transparent with your customer and set out at the beginning that you're sharing their data with the company

that is providing the warranty. But, as with every other supplier, you do need to make sure that you're happy that the company giving the warranty is handling the data properly. Part of your due diligence is to make sure that your suppliers are compliant – if they are based in the EU then they too will be subject to this legislation.

What do I do if a client ask me for a service that requires me to share their information with a 3rd party?

If a client asks you to perform a task for them that requires you to share some of their information with a 3rd party, for example if you are getting quotes on behalf of your client, ideally you'll get this request in writing but if it's a verbal request then just keep a note that they have asked you to do this.

Systems and processes

Is there any difference between handling written or digital data?

No, you have the same obligations for paper or digital information. Remember it's about transparency and being sensible so think about how you can prove that you are holding the data securely and doing the right thing with it. Also think about the obligations you have to an industry or other regulatory body that might set parameters on what information you need to keep about your business activities.

What measures do I need to take to secure my systems?

One of the obligations of the legislation is that you must hold personal data securely so you need to have software, physical security and policies in place to do this. Each business will have a different solution depending on the type of data that you hold and the infrastructure that you have in your business. Remember that you need to be able to evidence what you have done to protect your data that includes all the places where you hold data including your computer. There is more help on keeping your systems secure on these pages.

I use an online system to hold client data and my accounts

- what do I need to do ?

You need to be satisfied that any online provider you use is compliant with the data protection legislation so ask them about their security policies and make sure that you are comfortable that they are adequate. Many of these platforms will have a security policy statement that you can access through your subscription, but if you can't find this then send them an email request. One of the things to confirm is the physical location of the server that the data is sitting on as this will influence the regulations under which you data is held and be aware that US companies do not work under GDPR although they have a voluntary scheme called the US Privacy Shield which is compliant with EU legislation. If you are not happy with the policies that your provider has in place then look for another!

Do I have to have encrypted email messages?

The regulator won't mandate the systems or security that you use to keep your data secure but your customers or suppliers might do so.

What's the value of Cyber Essentials in relation to GDPR?

If you are a States of Jersey supplier then you will be asked to achieve Cybers Essentials accreditation. This is a policy decision that the States have made to ensure their suppliers are putting appropriate measures in place to secure the information they hold. Cyber Essentials is one mechanism to do this and therefore a worthwhile exercise for any company holding sensitive date.

Working with suppliers

When do I need a supplier agreement to be in place?

If you are sharing personal information with your suppliers then you need to be satisfied that they are also compliant with data protection legislation so see what agreement you already have in place. If you don't think these are adequate than revise them are introduce new ones if there is nothing in place.

What's the difference between data sharing and data

processing?

- Data sharing agreement = you share data with another controller for a common purpose
- Data processing agreement = you hand over data to another organisation to process it for you

Marketing

What if I want to keep talking to clients?

If you want to keep data about clients so you can tell them about other services then you need to ask them if that's ok. If they are happy to keep hearing from you then you can keep them on a mailing list.

Do I need to get consent for holding email data for marketing purposes?

The view in Jersey is that reconsenting is not necessary if people consented to being on your database when they originally signed up. However, one thing you will need to do is to make sure that your evidence of consent is compliant and that you update the information you hold about people so a recommendation is to do an annual review of your mailing lists to make sure that the people on your database are still happy to receive your mailing and that the information you have is accurate.

My website it a simple landing page/magazine site with my contact details but no links or forms, so I'm not collecting data. I assume data protection doesn't apply to my site?

Although you aren't collecting information directly from your website visitors, if you are using cookies or tracking their activity on your site in any way then you are collecting data about them. If you use Google Analytics and Cookies to help manage your site then you should have a Privacy Notice explaining this on the site. If you don't look at any of these reports then you should consider disabling them. Don't collect information about individuals if you don't need to.

Mailing lists

What do I need to do regarding mailing lists?

Firstly, establish that you obtained the information you have on the list lawfully, that is, from the individuals themselves, so if you have data about them collected by other means, buying a mailing list for example, you will need to go back to them and check they are happy for you to continue holding/using their data. Then you need to check they have all consented to being on your mailing list. How have they interacted with you? What are their expectations on how you use their data?

The only personal data I have is names and emails for a mailing list, what do I need to do?

Here are a few things you need to consider to make sure you email marketing is compliant:

- You need to make sure that you a processing the names and/emails lawfully and using one of the 5 legal bases. For many marketing activities you may wish to think about relying on either consent or legitimate interests as the legal basis to send your marketing information.
- If you use consent to send emails to the people who are on your list you should record this – maybe a tick box on an order form, a sign up form from your website or an email requesting or accepting to go on your mailing list. Keep it simple and easy to review/amend as necessary.
- If you use legitimate interests (so you don't have consent from the individuals directly but you consider that you have a legitimate reason to email them e.g. they are an existing client and you want to tell them about a new product) then you need to make sure that your privacy policy is very clear that this is the legal basis you are relying on to contact them.
- Tell them what you will be emailing them about when they sign up
- Make it easy for people to unsubscribe from the list and when they do take them off the list straight away

That's it.

What about enforcement?

How is all this being enforced?

In Jersey the approach is very much hand holding to make sure businesses have everything they need to be compliant. If businesses get it badly wrong or ignore advice then these will be the ones that are focused on first. The approach here is very much about making sure data protection works for everyone and the enforcement aspects of the role will kick in when something goes wrong.

Relevant Links

- Jersey Office of the Information Commissioner
- IOC UK – Data Protection Self Assessment
- Data Protection Definitions
- Data Protection for SMEs
- Data Protection Registration
- GDPR - What will it mean for your business?