Ardent Chambers

SMEs:

GDPR IMPLEMENTATION DE-MYSTIFIED

DATA PROTECTION

AND A BRIEF INTRODUCTION TO GDPR

What is GDPR? The General Data Protection Regulation (GDPR) is an EU Regulation designed to seek to give greater control around and protection to personal information. In Jersey the requirements of the GDPR will be implemented by two new data protection laws, the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018.

Link 1: For more general information on GDPR go to: www.thinkgdpr.org or www.oicjersey.org

Link 2: Further small business guidance is available here: www.ico.org.uk/for-organisations/business/

Link 3: www.oicjersey.org/wp-content/uploads/2018/04/2018.04.11-Guidance-for-SMEs.docx.pdf

"The new European General Data Protection Regulation (GDPR) is almost upon us, and with it brings about the biggest reform in data protection regulation ever seen. As the Authority charged with regulating the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018, we are acutely aware of the impact of these changes upon local businesses, and in particular those small and medium-sized enterprises that make up the large majority of our business community.

We cannot emphasise enough the importance of good information governance and having robust processes in place to protect the personal information you hold. However, we also acknowledge that for many SMEs, meeting compliance with the regulations may seem both a daunting and potentially costly exercise. With this in mind, we are here to support you and work with you wherever possible to encourage a positive culture of compliance and good information handling practice within your organisation."

- Paul Vane, Acting Information Commissioner Jersey

GDPR COMPLIANCE

What does GDPR apply to?

Data protection requirements apply to data about living persons. 'Personal data' is data that relates to a living person where that person can be identified from the data alone or in conjunction with other data in your possession or likely to come into your possession.

'Special category data' is a subsection of 'personal data' about a living person that is particularly sensitive and includes information about a person's:

(a) The racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) The genetic or biometric data that is processed for the purpose of uniquely identifying a natural person;
(c) The data concerning health;
(d) The data concerning a natural person's sex life or sexual orientation; or
(e) The data relating to a natural person's criminal record or alleged criminal activity.

GDPR only applies to 'personal data' and 'special category data'.
Examples of 'personal data' and 'special categories of data' include: telephone number, email address, date of birth, marital status, social security number, health information, criminal conviction information, banking information, height/weight, photographs, IP addresses and browser cookies.

GDPR does not apply to every piece of data that you would hold as a business. Some of your data will not relate to individual persons but, for example, will be about the operation of your business and some of it may even be publicly available i.e. because it is posted on social media forums.

I have a business, does GDPR apply to me?

GDPR doesn't apply to the processing of data for personal reasons or to run a household. However, if you are running a business or organisation from Jersey (either due to being incorporated or resident there) then you are going to hold or process personal information about people - even if it is simply their names and telephone numbers or email addresses.

When does GDPR come into force?

25 May 2018.

I have a business, does GDPR apply to me?

GDPR doesn't apply to the processing of data for personal reasons or to run a household. However, if you are running a business or organisation from Jersey (either due to being incorporated or resident there) then you are going to hold or process personal information about people - even if it is simply their names and telephone numbers or email addresses.

What happens if I don't comply?

The Data Protection Authority in Jersey will have new enforcement powers, including the ability to search/seize, investigate and issue fines for breaches. Under Jersey's legislation the fines are not to exceed £300,000 or 10% of a person's total annual turnover or gross income for the preceding financial year, whichever is the highest - up to £10,000,000.

What is a 'data controller' and 'data processor' and which am I?

A 'data controller' is someone who determines the purpose and manner in which personal data is to be processed. A 'data processor' is someone who is not an employee of a data controller but who receives personal data from the data controller or on behalf of the data controller and then processes it, for example outsourced activities.. Processing includes:

(a) Organising, adapting or altering the data;
(b) Retrieving, consulting or using the data;
(c) Disclosing the information or data by transmission, dissemination or otherwise; or
(d) Aligning, combining, clocking, erasing or destroying the data or information.

It is important to know in respect of any personal data that you hold, whether you are the controller, joint controller or processor. It is most likely you will be both a controller and processor but in respect of different types of personal data. For example if you receive payroll information from your employees such as banking details and then send it to an external payroll provider, then you are the data controller and the payroll provider is the data processor. If you use an external IT consultant then they are highly likely to be a data processor, whereas you will be the data controller. It is also possible to be a joint controller of personal data and divide responsibilities for that particular personal data between the joint controllers, with the exception that the person to whom the data relates to can request their personal data from either data controller where there are joint controllers. It is the responsibility of the data controller under law to implement proportionate technical and organisational measures to ensure processing is performed in accordance with the requirements.

Do I need a data protection officer?

If you are a public authority or control/processing special category data on a large scale as part of your core activities, then you must appoint someone to be your data protection officer ("DPO"). The role of the DPO is to keep your organisation or business informed about GDPR, monitor compliance with the data protection requirements and be the first point of contact for both the Data Protection Authority and for those whose data you process (employees and clients/customers). It is possible to outsource this function to a provider or join together with a group of undertakings and appoint a single data protection officer. If you do need a DPO, then you have until 25 November 2018 to appoint one.

Can I use other people's data?

In order to control or process the data of others lawfully you will need to be registered with the Data Protection Authority in Jersey. If you are already registered with Office of the Information Commissioner in Jersey as a data controller then your current annual registration will roll over on 25 May 2018, when GDPR comes into force. If you are not already registered as a data controller then you will need to be by 25 May 2018. If you solely process data on behalf of others as a data processor and do not act as a data controller in anyway then you need to be registered by 25 November 2018.

In addition to being registered, you also need to have a lawful reason to process a person's data. The lawful reasons that businesses usually rely upon are either that they controlling or processing the data:

(a) with the consent of the person whose information it is;
(b) in accordance with a contract;
(c) under a legal obligation; or
(d) in furtherance of their legitimate interests i.e. usual course of business.

What constitutes a data breach?

Data breaches need to be reported to the Data Protection Authority within 72 hours of you becoming aware of the breach. It is therefore important to have in place the right processes to detect, investigate and report breaches when they happen and for any employees to be clear on that process. Further guidance has been issued on the position Jersey will take to breach reporting and can be found at: www.oicjersey.org/wp-content/uploads/2018/04/2018.03.13-Guidance-on-Breach-Reporting.pdf. The Jersey legislation requires that a breach shall be reported if it poses a risk to an individual's rights or freedoms – i.e. could result in discrimination, damage to reputation, financial loss or loss of confidentiality. If there is a high risk of impact to the rights or freedoms of individuals, then those individuals also need to be notified personally. This has to be determined on a case by case basis. To give an example the loss of customer banking details would need to be reported to both the Data Protection Authority and individuals concerned but the stealing of an internal employee telephone list would probably not require reporting at all.

A breach notification should state where possible:

(a) The nature of the personal data breach;
(b) Categories or approximate number of people concerned;
(c) Categories and approximate number of personal data records concerned;
(d) Name and contact details of DPO or other contact point;
(e) Likely consequences of the breaches; and
(f) Any mitigating measures taken or to be taken to address the breach.

Can an individual find out what information I hold about them?

A subject access request can be made by an individual who wishes to see what personal data an organisation or business holds about them. A person is only entitled to see their own personal data, not the data of others unless they have the appropriate authority to do so, such as lawyer on behalf of client or parent on behalf of child. A person who makes a subject access request is entitled to know:

(a) whether you are holding or processing any personal data of theirs;
(b) be given a description of the personal data and the reasons it is being held or processed;
(c) given the information contained in the personal data and the details and source of the data, if available. Note the person making the request is entitled to the underlying personal information, not the documents it is contained in; and
(d) request information about the reasoning behind any automated decisions, e.g. computer generated decision to grant or deny credit.

Under the new requirements, a subject access request must be responded to within 4 weeks of receipt. It is possible to extend the time frame for a response to 8 weeks if there are several requests made or if they are large in nature but the data subject must be informed within 4 weeks of that extension and the reasons for it. In most cases no fee can be charged for providing information in response to a subject access request, unless the request is manifestly unfounded or excessive. This is a change from the previous position where you could charge up to £10 for responding to a subject access request.

As an SME, how can I comply with GDPR quickly and cost efficiently?

At its simplest, the key is to take this two stage approach:

(a) Map your own data – also known as a 'data audit'; and
(b) Update key policies, procedures and security precautions in response to your data mapping exercise.

There is no one size fits all approach to GDPR because your business/ organisation will receive and deal with personal and sensitive personal data in its own way. Whilst you can gain inspiration from what others are doing, the data mapping exercise must focus on how your business handles its data about others.

How do I map my data?

To map the personal and special category data that you control or process you need to look at how you receive such information, how it comes to your business/organisation and then how you share, retain and secure it.

For SMEs a simple spreadsheet can work. Here is an outline for a potential spreadsheet with some examples:

How data received/ Why obtained	Data type	Personal or special category data	Basis for processing	Controller/ Processer	Where data held	Retention period	Security controls	Shared with who (additional details if shared outside EEA)
Website Enquiry	Name Email Address	Personal data	Legitimate interest	Controller	On data base/ spreadsheet	X period of time in order to reply to query If they become a client/ customer, retained for X period	Pen testing of website Security controls around data base have been confirmed by provider to apply security standard XYZ	Not shared, unless have consent of the client/ customer
Telephone Call requesting services	Name Address Telephone Number Health Concern	Personal data and Special Category Data	Contract/ Legitimate Interest	Controller	Data base Or Word document (held in cloud)	X period after last consultation	Information entered into word doc. or onto data base Security controls around data base or cloud provider have been confirmed to apply to XYZ security standard	

A word on retention:

Under data protection requirements personal data retained must be relevant and up to date. It is not permissible to keep personal data 'just in case' or because 'you might need it one day'. For some businesses, they have professional rules about retaining certain information for prescribed periods. This can make retention periods in some areas simpler, where that is the case. For other businesses there are no such requirements and it is a case of exercising common sense having regard to your actual business need to retain personal data. Remember that the more personal or special category data that you have in your possession, the greater your needs are going to be to keep it secure. Less is more! Ask yourself – what am I keeping this for and how long do I need it to fulfil that purpose? For example you might have a policy to keep an employee's full personnel file for a set period after they have left your organisation, with the exception of information necessary to provide references or contact details that is retained for a longer period. For clients or customers, you might retain their information for a set period of time after a service/product is last provided to them and then only retain (if they have positively given their consent) their contact details to provide them with marketing information thereafter.

I've done my data audit, what documents do I need to produce/ update to be compliant?

There are essentially 4 key policies/documents that you need to produce/ update in response to your data mapping exercise, they are your:

(1) Privacy Statement;
(2) Consent Clauses (including marketing consents);
(3) Data Protection Policies (internal and external); and
(4) Third Party Agreements.

(1) Privacy Statements

Any Privacy Statement must tell your customers/clients simply and in easy to understand language:

(a) who you are and what you do;
(b) what information of theirs you hold and why;
(c) how you use their information, share it and store it;
(d) how long you retain it for;
(e) where the data was obtained from (if not direct from the data subject);
(f) if information is sent outside of European Economic Area (EEA) the reasons for that and any safeguards in place;
(g) how they can request their data (i.e. make a subject access request) and request that information is deleted or rectified (unless these points are covered elsewhere in your documentation); and
(h) contact details for DPO (if needed) and their right to complain to the Data Protection Authority.

It is perfectly acceptable to have slightly different rules and therefore a different explanation in your policy statement around retention for particular pieces of information, documents or data, if your business approach necessitates that. The point is that you need to be clear with your clients/customers/employees so that if someone provides a piece of personal data to you, they then have clarity over what will happen to it, where it will be stored and who it is shared with. If personal data Is shared outside of the EEA, then you need to explain that and the additional safeguards you have put in place, as such information once transferred will not be protected by the same standards as required under GDPR.

Privacy statements are popping up everywhere. If you start looking around you will see that your banks, doctors surgery, utility companies and others have probably produced them already. These statements can provide inspiration for producing your own privacy statement that reflects your own business practice. Below are some examples of privacy statements that you can find online. You should include sections on your use of website cookies and social media plugins, if you utilise them. Most businesses are putting their privacy statements on their websites and then either providing a paper copy of them to customers as a standard (or on request) including a cross reference to their privacy policy in their usual terms and conditions/initial contract with a client.

Link 1: www.getharvest.com/privacy-policy
Link 2: www.lboro.ac.uk/alumni/privacy/
Link 3: www.mhmk-international.org/privacy.html
Link 4: www.tfgm.com/privacy-policy
Link 5: www.webreality.co.uk/privacy-policy/
Link 6: www.pentagon.je/privacy-policy/

For further information on Privacy Statements look at:
Link 7: www.ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

(2) Consent Clauses

If you are relying upon a person's consent to process personal data (instead of contract or legitimate interest for example) then you must have a clear way for those whose data you are obtaining to indicate that they agree not just to you obtaining that information but the different uses of it. If you currently use consent forms for people to confirm they are happy that you control or process their data, then it is likely you will need to amend those forms to get multiple consents to the different uses of the person's data. i.e. separate consent to provide services to the person from consent to receive marketing material or updates/alerts. A tip here is that if you go back to your Privacy Policy and look at the different ways that you have explained you use a person's personal data listed and then tie your consents into that list, you should have everything covered.

Example:

Here at [organisation x] we value your privacy and we will only use your personal information to administer your account and provide products and services to you. However, from time to time we would like to contact you with details of:

(a) Other services we provide;
(b) Updates; or
(c) Competitions.

Please tick against each box that you would wish to receive information for.

An area of frequent concern for businesses is how they manage regular marketing approaches under GDPR, for example sending out email news alerts. In order to market to someone, they need to have clearly opted in and agreed to receive that marketing material. It is not sufficient to have pre-ticked boxes anymore. An individual has to positively opt-in (i.e. tick the box/click a button themselves). Here is an example of a business listing its different newsletters and asking those subscribing to clearly opt into their preferences:

Link 1: www.social.quintevents.com/quintevents-newsletter-subscription

If you have an existing mailing list, the key to whether you can continue to use it after GDPR is how you gained people's consent to be on that marketing list in the first place. If they positively opted in at the time, that would meet the GDPR requirements. If you are unsure or used pre-ticked boxes then you will need to regain consent to be able to mail those on your mailing list post GDPR. It is not enough to ask an existing member of your mailing list to simply unsubscribe, if they didn't positively opt in when you first signed them up to your mailing list. However, it is good practice to have an unsubscribe option for those who have positively opted in to receive your marketing material, so they can opt out at a later date if they wish.

(3) Data Protection Policies

Policies need to cover both internal and external angles. The internal angle is about ensuring that you have a clear internal policy for dealing with subject access requests, deleting or rectifying data and a process for handling a data breach, should it occur. This is often contained in an Employee Handbook or similar document. The external aspect is about how you communicate to those whose data you control or process their rights in respect of the data you hold on them. This can be a short 1-2 page document handed out on request or available on your website or as part of your Privacy Policy. The Policy, wherever contained, should explain to individuals:

(a) how they can access the personal data you hold on them or have it rectified or deleted;
(b) how they can make a subject access request for a copy of the personal data about them that you hold, which will be provided within 4 weeks of the request being received unless there is a valid reason for either an extension in the time to respond or a refusal to respond;
(c) their right to complain to the Data Protection Authority if unhappy; and
(d) what you will do in the event of a data breach and how the customer/client will be notified, if sufficiently serious.

Imagine that you are a new employee coming into your business with no GDPR experience – do you understand from the internal policy what is required of you around other people's data? If you disclose someone else's data by mistake, do you know what to do? If someone asks for their data, do you know what the process is for them to obtain it? On the flip side, if I have signed up as a new client/customer – do I understand how to access my data or what you will do if you lose my data?

(4) Third Party Agreements

Third party agreements apply to two scenarios. Firstly, where you are the data controller and someone else processes data for you. Secondly, where you are the data processor for someone else who is the data controller.

A key point is that GDPR makes written contracts between controllers and processors a requirement, rather than just a way of demonstrating compliance. It is not just a requirement to have written contracts in place but they must also contain certain specified terms as a minimum. For quick checklists on the terms your third party agreements need to cover look at:

Link 1: www.iapp.org/media/pdf/resource_center/GDPR-Checklist-for-Third-Party-Agreements__Final_.pdf

Link 2: www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Security

We are not security experts at Ardent Chambers but if you are responsible for people's personal data it is important to think about how you store and transport/send it. Do your systems have passwords that are regularly changed/randomly generated? Do you encrypt email containing sensitive or personal data? If you keep physical copies of such documentation, how are they kept secure in the office and when you travel? Do you know the security perimeters/standards that are applied to any systems that you are using and where the systems are based (in EEA or outside)?

The new data protection legislation requires controllers and processors to implement technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage. The level of measures undertaken should be proportionate to the business size and operations but the legislation lists measures such as encrypting data, restoring data in the event of a physical or technical incident and process for testing and evaluating organisational measures.

For wider information on keeping data secure look at:

Link 1: www.ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Link 2: www.cyberessentials.ncsc.gov.uk

Link 3: www.gov.je/StayingSafe/BeSafeOnline/ProtectYourBusinessOnline/pages/cyberessentials.aspx

Products that are free/well priced that might help are Apps and services that can encrypt data when you send it by email and that randomly generate passwords such as Galaxkey www.galaxkey.com and the Google Authenticator App.

A common worry from businesses is also how to manage storage and retention of emails, which may contain personal information. Using tag, categorisation and expiration dates settings within your email service - so that emails containing personal information can be tagged and deleted on a specified date - can help with this.

GDPR quick compliance checklist

Have you:

- → Completed your data audit;
- → Updated or created: privacy notices, consent notices (including marketing consents and mailing lists) and data protection policies;
- → Reviewed contracts or terms and conditions with third parties;
- → Trained employees in GDPR and introduced any new changes in policies and procedures to employees;
- → Put in place a DPO, if needed; and
- → Given thought to the security measures that you have in place around personal data and whether further security measures are needed.

Contact details:

The aim of this guide is to enable SME's to implement their own GDPR compliant processes and documentation. However, if you do require further legal help and support, please contact:

Caroline Dutot
Ardent Chambers
cdutot@ardentchambers.com
(+44) 1534 481809

www.ardentchambers.com/advocate-caroline-dutot/

Office of the Information Commissioner
(+44) 1534 716530
General enquiries: enquiries@OICJersey.org
Breach reporting: breach@OICJersey.org

www.oicjersey.org

Ardent Chambers

SMEs:

GDPR IMPLEMENTATION DE-MYSTIFIED