OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE:
GUIDE FOR SMEs

OFFICE OF THE INFORMATION COMMISSIONER

Guidance Note

Guide for Small and Medium Sized Enterprises ("SMEs")

Data Protection (Jersey) Law 2018

What will the GDPR and Data Protection (Jersey) Law 2018 (DPJL) mean for your organisation?

- Both the GDPR and DPJL come into effect on 25th May 2018.
- The GDPR is applicable to:
  - EU organisations processing personal data of EU individuals;
  - Non-EU organisations offering goods/services to EU individuals;
  - Non-EU organisations monitoring the behaviours of individuals in the EU.
- The DPJL is applicable to any organisation holding or using personal information about customers based in Jersey. It reflects the provisions and principles of the GDPR.
- The core aims of the GDPR and DPJL are to protect the rights and freedoms of individuals in respect of their personal information. Organisations (data controllers and data processors) have obligations under both laws to respect those rights under the general principles of transparency and accountability, to the extent that such legislation applies to them.

This guide and the accompanying checklist have been designed to assist SMEs based in Jersey, who may not have access to extensive planning and legal resources. Using this guide, along with our twelve-step guide, will help those businesses in particular to prepare for a business future that is data-protection compliant.

If you process personal data as part of your business, the DPJL will apply to you and the GDPR might apply to you if you fulfil the criteria set out above.

It is important to remember that:

- Customer AND employee data is personal data
- Simply storing personal data electronically or in hardcopy constitutes 'processing' personal data
- The DPJL (and where applicable, the GDPR) applies to both controllers AND processors.

Key definitions

GDPR: The General Data Protection Regulation (2016/679) is the new EU Regulation on Data Protection, which will come into effect on the 25th May 2018.

Personal Data: Information relating to a living individual who is, or can be, identified by that information, including data that can be combined with other information to identify an individual. This can be a very wide definition, depending on the circumstances, and can include data which relates to the identity, characteristics or behaviour of an individual or influences the way in which that individual is treated or evaluated.

Processing: means performing any operation or set of operations on personal data, including:

- obtaining, recording or keeping data;
- organising or altering the data;
- retrieving, consulting or using the data;
- disclosing the data to a third party (including publication); and
- erasing or destroying the data.

Data Controller: A Data Controller is the person (in the case of a sole trader) or organisation who decides the purposes for which, and the means by which, personal data is processed. The purpose of processing data involves 'why' the personal data is being processed and the 'means' of the processing involves 'how' the data is processed.

Data Processor: A person or organisation that processes personal data on the behalf of a data controller, for example, outsourced activities such as IT provision, cloud providers, human resources. They are not employees of the data controller. They can only act on the written instructions of the controller.

Data Subject: A Data Subject is the individual the personal data relates to.

Data Protection Impact Assessment (DPIA): A DPIA describes a process designed to identify risks arising out of the processing of personal data and minimisation of these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance, with the DPJL and GDPR. DPIAs should be carried out before any processing of data takes place.

DPJL: The Data Protection (Jersey) Law 2018, which comes into force on 25th May 2018. It replaces the Data Protection (Jersey) Law 2005.

Lawful basis for processing personal data: In order to process personal data you must have a lawful (legal) basis to do so. The lawful grounds for processing personal data are set out in Schedule 2 of the DPJL. These include:

- where you have the consent of the individual;
- where it is necessary for performance of a contract;

- where it is necessary to protect the vital interests of a person;
- where it is necessary for the performance of a task carried out in the public interest; or in the legitimate interests of company/organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject).

Controllers can rely on any of the conditions for processing set out in Parts 1 and 2 of Schedule 2.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Additionally, Schedule 2 (Part 2) of the DPJL sets out the lawful bases for processing of special category (sensitive) personal data. If you want to process special category data, you need to identify the lawful basis in Part 2 of Schedule 2.

You need to work out the legal basis before you start processing and document your thinking.

Retention Policy: How long will your organisation hold an individual's personal data? This will be influenced by a number of factors. There may be legal requirements on your organisation, depending on your business type (e.g. General Medical Council or JFSC rules). Keep the data for the least amount of time that you can in accordance with the requirements of your business, store it securely while it is in your possession and make sure to delete it fully and safely at the appointed time.

Special Category Data: This is defined in Article 1 of the DPJL as data 'which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or data relating to a person's criminal record or alleged criminal activity'. If you want to process Special Category Data you need to be able to also identify one of the lawful bases in Schedule 2 Part 2 of the DPJL.

Consent: Article 11 of the DPJL has increased the conditions needed for consent as a legal basis for data processing to be valid. It is now necessary to consider whether consent was unambiguous, informed and freely given and the data subject must have the opportunity to withdraw consent for processing at any time.

Consent should not be assumed (no more pre-ticked boxes) and must be obtained before data processing begins (e.g. through Privacy Notices). There must be a positive, affirmative action by the data subject for consent to be valid.

It also requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

If you offer online information services to children (i.e. purchasing of apps), it is necessary to ensure that you can verify their age and the consent of someone having "parental responsibility" must be obtained if the child is under the age of 13.

The key steps you need to take

- Identify what personal data you hold (this can be achieved by setting out the information listed in Article 14 of the DPJL or for smaller companies a tailored process such as the accompanying template that identifies details of personal data held).

- Conduct a risk assessment of the personal data you hold and your data processing activities (Article 14(5) DPJL).

- Implement appropriate technical and organisational measures to ensure data (digital *and* paper files) is stored securely. The security measures your business should put in place will depend on the type of personal data you hold and the risk to your customers and employees should your security measures be compromised.

- Know the legal basis you rely on (consent? contract? legitimate interest? legal obligation?) to justify your processing of personal data (Schedule 2 DPJL).

- Ensure that you are only collecting the minimum amount of personal data necessary to conduct your business, that the data is accurate and kept no longer than is needed for the purpose for which it was collected (Article 8 DPJL).

- Be transparent with your customers about the reasons for collecting their personal data, the specific uses it will be put to, and how long you need to keep their data on file (e.g. notices on your website or signs at points of sale) (Article 12 DPJL).

- Establish whether or not the personal data you process falls under the category of special categories (sensitive) of personal data and, if it does, know what additional precautions you need to take (Schedule 2 (Part2) DPJL).

- Decide whether you will need to retain the services of a Data Protection Officer (DPO) (Article 24 DPJL). The DPJL allows you to outsource this function, however you should be sure to check your DPO has the skills and time to fulfil their statutory obligations under the DPJL.

- Have appropriate procedures in place to facilitate requests from individuals wishing to exercise their rights under the DPJL, including rights of access, rectification, erasure, withdrawal of consent, data portability and the right to object to automated processing (Articles 27 to 38 DPJL).

- Where appropriate, have up-to-date policy/procedure documents that detail how your organisation is meeting its data protection obligations.

- Train your staff so that they know why it is important for data to be dealt with properly, how to do that and what they need to do/who they need to speak to if something goes wrong.

- Have appropriate procedures in place to deal with any breach. You will ordinarily have 72 hours from date of notification of the breach to report the matter to the Authority so make sure you know what needs to be done, and by whom. You might also need to tell data subjects about what has happened.

A risk based approach to compliance

When your organisation collects, stores or uses (i.e. processes) personal data, the individuals whose data you are processing may be exposed to risks. It is important that organisations that process personal data take steps to ensure that the data is handled legally, securely, efficiently and effectively in order to deliver the best possible care.

What risk does the information you hold pose to your customers?

The risk-profile of the personal data you hold should be determined according to:

- the personal data processing operations carried out;
- the complexity and scale of data processing;
- the sensitivity of the data processed; and
- the protection required for the data being processed.

For example, where a data processing activity is particularly complex, or where a large volume or sensitive data is involved (i.e. an internet, health, financial or insurance company), this would attract a higher risk rating than routine personal data that relates solely to employee or customer account details.

Think of the potential harm to your customers.

It is useful to look at the tangible harms to individuals that your organisation needs to safeguard against. These may include processing that could lead to:

- Physical, material or non-material damage;
- Discrimination;
- Identity theft or fraud;
- Financial loss;
- Reputational damage;
- Loss of confidentiality protected by professional secrecy;
- Unauthorised reversal of pseudonymisation;
- Any other significant economic or social disadvantage.

TIP: Conduct a risk-assessment to improve awareness of the potential future data protection issues associated with a project. This will help to improve the design of your project and enhance your communication about data privacy risks with relevant stakeholders.

Data protection by design and by default

The DPJL and GDPR provide for two crucial concepts for future project planning: **Data Protection By Design** and **Data Protection By Default**. While long recommended as good practice, both of these principles are now enshrined in the DPJL (Article 15).

Data Protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Protection by default means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is *necessary* for each specific purpose of the processing should be gathered at all.

Data Protection Impact Assessment (DPIAs)

Under the DPJL, a Data Protection Impact Assessment (DPIA) is a mandatory pre-processing requirement where the envisaged project/initiative/service involves data processing which "is likely to effect in a high risk to the rights and freedoms of natural persons." (Article 16 DPJL).

This is particularly relevant when a new data processing technology is being introduced in your organisation. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still best practice and a very useful tool to help data controllers demonstrate their compliance with data protection law. DPIAs are scalable and can take different forms, but the DPJL sets out the basic requirement of an effective DPIA.

Data protection risk register

Maintaining a data protection risk register can allow you to identify and mitigate against data protection risks, as well as demonstrate compliance in the event of a regulatory investigation or audit.

DPJL readiness checklist tools:

In addition to the general checklist below, the following pages will take organisations through more detailed questions in the areas of:

- Personal data
- Data subject rights
- Accuracy and retention
- Transparency requirements
- Other data controller obligations
- Data security
- Data breaches
- International data transfers

The following tables will assist organisations in mapping the personal data that they currently hold and process, recording the lawful basis on which the data was collected, and specifying the retention period for each category of data. Carrying out this exercise will help identify where immediate remedial actions are required in order to be compliant with the DPJL (and, where appropriate, the GDPR).

General checklist:

Categories of personal data and data subjects	**Elements of personal data included within each data category**	**Source of the personal data**	**Purposes for which personal data is processed**	**Legal basis for each processing purpose (non-special categories of personal data)**	**Special categories of personal data**	**Legal basis for processing special categories of personal data**	**Retention period**	**Action required to be compliant?**
List the categories of data subjects and personal data collected and retained e.g. current employee data; retired employee data; customer data (sales information); marketing database; CCTV footage.	*List each type of personal data included within each category of personal data e.g. name, address, banking details, purchasing history, online browsing history, video and images.*	*List the source(s) of the personal data e.g. collected directly from individuals; from third parties (if third party identify the data controller as this information will be necessary to meet obligations under Article 12 DPJL).*	*Within each category of personal data list the purposes for the data is collected and retained e.g. marketing, service enhancement, research, product development, systems integrity, HR matters, advertising.*	*For each purpose that personal data is processed, list the legal basis on which it is based e.g. consent, contract, legal obligation (Schedule 2 DPJL).*	*If special categories of personal data are collected and retained, set out details of the nature of the data e.g. health, genetic, biometric data.*	*List the legal basis on which special categories of personal data are collected and retained e.g. explicit consent, legislative basis (Schedule 2 (Part 2) DPJL).*	*For each category of personal data, list the period for which the data will be retained e.g. one month? one year? As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.*	*Identify actions that are required to ensure all personal data processing operations are compliant e.g. this may include deleting data where there is no further purpose for retention.*

Personal data:

	Question	Yes	No	Comments/Remedial Action
Consent based data processing (Article 11 DPJL)	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of statement or a clear affirmative action?			
	If personal data that you currently hold on the basis of consent does not meet the required standard under the DPJL, have you re-sought the individual's consent to ensure compliance with the DPJL?			
	Are procedures in place to demonstrate that an individual has consented to their data being processed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
Children's personal data (Article 11(4) DPJL)	Where information society services are provided to a child, are procedures in place to verify age and get consent of a parent/ legal guardian, where required?			

Data Subject Rights:

	Question	Yes	No	Comments/Remedial Action
Access to personal data (Article 28 DPJL)	Is there a documented policy/procedure for handling Subject Access Requests (SARs)?			
	Is your organisation able to respond to SARs within one month?			
Data portability (Article 34 DPJL)	Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format?			
Rectification and erasure (Articles 31 and 32 DPJL)	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
Right to restriction of processing (Article 33 DPJL)	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
Right to object to processing for direct marketing purposes, public functions or legitimate interests (Articles 35 and 36 DPJL)	Are individuals told about their right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest?			
	Are there controls and procedures in place to halt the processing of personal data			

	where an individual has objected to the processing?			
Profiling and automated processing (Article 38 DPJL)	If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected?			
	Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?			
Right to object for historical or scientific purposes (Article 37 DPJL)	Is the lawfulness for processing based solely on the need to process for archiving or research purposes?			
Handling of requests by data subject in relation to their rights (Article 27 DPJL)	Have you taken appropriate action as is required within the required timeframes?			

Accuracy and retention:

	Question	Yes	No	Comments/Remedial Action
Purpose limitation	Is personal data only used for the purposes for which it was originally collected?			
Data minimisation	Is the personal data collected limited to what is necessary for the purposes for which it is processed?			
Accuracy	Are procedures in place to ensure personal data is kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Retention	Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected?			
Other legal obligations governing retention	Is your business subject to other rules that require a minimum retention period (e.g. medical records/tax records)?			
	Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies?			

Duplication of records	Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records?			

Transparency requirements:

	Question	Yes	No	Comments/Remedial Action
Transparency to customers and employees (Articles 12 DPJL)	Are service users/employees fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form using clear and plain language?			
	Where personal data is collected directly from the individuals, are procedures in place to provide the information listed at Article 12 of the DPJL?			
	If personal data is not collected from the subject but from a third party (e.g. acquired as part of a merger) are procedures in place to provide the information listed at Article 12 of the DPJL?			
	When engaging with individuals, such as when providing a service, sale of a good or CCTV monitoring, are procedures in place to proactively inform individuals of their rights under the DPJL?			
	Is information on how the organisation facilitates individuals exercising their DPJL rights published in an easily accessible and readable format?			

Other data controller obligations:

	Question	Yes	No	Comments/Remedial Action
Processor Agreements (Articles 19 DPJL)	Have agreements with suppliers and other third parties processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included?			
Data Protection Officers (DPOs) (Articles 24 DPJL)	Do you need to appoint a DPO as per Article 24 of the DPJL?			
	If it is decided that a DPO is not required, have you documented the reasons why?			
	Where a DPO is appointed, are escalation and reporting lines in place? Are these procedures documented?			
	Have you published the contact details of your DPO to facilitate your customers/ employees in making contact with them?			
Data Protection Impact Assessments (DPIAs) (Article 16 DPJL)	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			

Data security:

	Question	Yes	No	Comments/Remedial Action
Appropriate technical and organisational security measures (Article 21)	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
	Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?			
	Is there a documented process for resolving security related complaints and issues?			
	Is there a designated individual who is responsible for preventing and investigating security breaches?			
	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
	Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained.			
	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			

Data breaches:

	Question	Yes	No	Comments/Remedial Action
Data Breach response obligations (Article 20 DPJL)	Does the organisation have a documented privacy and security incident response plan?			
	Are plans and procedures regularly reviewed?			
	Are there procedures in place to notify the office of the Data Protection Commissioner of a data breach?			
	Are there procedures in place to notify data subjects of a data breach (where applicable)?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches?			

International data transfers (outside the EEA) – if applicable:

	Question	Yes	No	Comments/Remedial Action
International data transfers	Is personal data transferred outside the EEA, eg. To the US or other countries?			
	Does this include any special categories of personal data?			
	What is the purpose(s) of the transfer?			
	Who is the transfer to?			
	Are all transfers listed – including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data, and who the recipient of the data is?)			
Legality of international transfers	Is there a legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses. Are these bases documented?			
Transparency	Are data subjects fully informed about any intended international transfers of their personal data?			

Additional information

Additional guidance is available on our guidance pages with more information on other aspect of the DPJL.

This guidance has been developed drawing on the Commissioner's experience. It will be reviewed and considered from time-to-time in line with new decisions by the Commissioner and/or the Jersey courts.

It is a guide to our general recommended approach, although each individual case will likely be different and will be decided on the particular circumstances of the case.

If you need any further information about this, or any other aspect of the DPJL, please contact us or see our website www.OICJersey.org.

Contact Us

Main office: +44(0)1534 716530
General email: enquiries@OICJersey.org
Website: www.OICJersey.org and www.thinkGDPR.org

Office address:

Brunel House
Old Street
St Helier
Jersey JE2 3RG

OFFICE OF THE INFORMATION COMMISSIONER