GDPR - What will it mean for your business?

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

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.

> **Download the GDPR Infographic**
> **GDPR For Smes**
> (540KB)

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.

Steps you need to take need to do to implement GDPR in your business

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. **GDPR Infographic – Do I or Dont I need a DPO**

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. **GDPR Infographic – Your GDPR Implementation plan**

Other useful sources of information.

Additional guidance is available on the Office of the Information

What else do I need to consider for GDPR?

Commissioner guidance pages with more information on other aspects 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 their 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 the Office of the Information Commissioner or visit www.OICJersey.org.

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

Office address: 2nd Floor,
5 Castle Street, St. Helier, Jersey JE2 3BT

Relevant Links

- Jersey's Information Commissioner
- IOC UK – Data Protection Self Assessment
- DPJL
- GDPR
- GDPR – A risk based approach to compliance
- Data Protection for SMEs
- Data Protection Definitions
- Data Protection – Frequently asked questions

Keep up-to-date with business information, news and events
sign up for the Jersey Business newsletter.

Subscribe →