GDPR – A risk based approach to compliance

Your business must ensure that the data is handled legally, securely, efficiently and effectively in order to deliver the best possible care.

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.

Download
6 Essential Steps to GDPR Compliance Infographic
(414KB)

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

It is useful to look at the tangible harms to individuals that your organisation needs to safeguard against. These may

harm to your customers

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).

Download
the DPJL Readiness Checklist
(40KB)

Relevant Links

- Jersey's Information Commissioner
- Data Protection for SMEs
- Data Protection Registration
- Data Protection – Frequently asked questions
- GDPR - What will it mean for your business?

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

Subscribe →