PREPARING FOR GDPR

YOUR NEXT STEPS

The key features of the General Data Protection Regulation and how you can start to prepare.

OFFICE OF THE INFORMATION COMMISSIONER
THE OFFICE OF THE DATA PROTECTION COMMISSIONER
www.dataci.org

Awareness

The GDPR will be in force across all EU Member States from May 2018. The Channel Islands have committed to enacting equivalent legislation at the same time and drafting will start early in 2017. This will serve to enhance the rights of citizens in this digital age as well as protect the free flow of data to the Islands by ensuring continued 'adequacy' status with the European Commission.

Action Required

- Board/senior management awareness and support is essential.
- Consider resource and procedural implications.
- Add GDPR to your risk register and inject data protection check points into all project management and budgeting processes.
- Task key people to keep up to date with developments.
- See our website for further information: www.dataci.org

Wider Scope

GDPR will apply to non-EU organisations processing the personal data of EU citizens, monitoring their behaviour or offering goods and/or services. Organisations established in more than one EU Member State must determine where their 'main establishment' is to identify the lead regulator. Non-EU organisations may be required to appoint a representative in an EU Member State. Data Processors will have specific obligations. This is important if you are a cloud provider or use their services. Updated definitions will capture more data than is currently the case.

Action Required

- Establish whether you have, or are likely to have, EU clients.
- Identify your 'main establishment' noting that there will be liability issues with this status.
- Identify whether you have information which does not currently fall within the definition of personal data but may do so under the GDPR.

Privacy Notices

Transparency of processing is a key element of GDPR compliance. It ensures individuals are clear about how their data are going to be processed and provides a greater degree of control over how such processing is to be carried out.

Action Required

Wherever you collect personal data you must provide detailed information to the individual, including:

- The purpose of and legal basis for the processing
- Details of recipients of the data
- Any third countries data are transferred to and safeguards in place
- Data retention periods
- Rights afforded to individuals in law
- The right to withdraw consent where consent has been relied upon for collection
- The contact details of the Data Protection Officer (if applicable).

Penalties and Data Breaches

The GDPR provides the regulator with wide enforcement powers and introduces significant fines for non-compliance. Individuals are also able to sue for compensation. It will be mandatory in most cases to report data breaches to the regulator immediately. You may also be required to notify the affected data subjects if there is risk or potential risk of harm.

Action Required

- Integrate data protection as part of corporate risk management
- Develop an internal breach management and reporting process.
- Review and update your policy for the investigation and handling of data breaches.
- If you are a data processor, or use the services of a data processor, ensure you have written contracts covering the data protection requirements. Understand what your liability is going to be.

Privacy by Design and DPIAs

Organisations will be required to 'build in' data protection compliance to all processing from the outset. Data Protection Impact Assessments (DPIAs) must be carried out where there is high volume and/or high risk processing. Documentary evidence of all such processes must be retained.

Action Required

- Engage with your data protection obligations at the initial phase of all projects involving personal data.
- Document data protection compliance including assessment of risk and steps taken in mitigation.

Data Protection Officers

Data Protection Officers (DPO's) will be mandatory for public authorities and for private sector organisations where the processing is considered high risk.

Action Required

- Identify an individual who can act as DPO for your organisation and make sure they are appropriately supported.
- Even if the Law does not require you to have one, it can provide your organisation with valuable expertise.

Subject Access Requests

The GDPR enhances the rights of individuals to access their personal data. Requests must be complied with within a month and you will no longer be able to charge a fee.

Action Required

- Ensure your records management systems and processes support the efficient discovery of information.
- Identify a point of contact to deal with subject access requests.
- Make details of your point of contact easily available.

What, where, why, how?

Any effective data governance strategy has to begin with a comprehensive data audit and this will help underpin the accountability aspect of compliance.

Action Required

Document detailed responses to the following questions:

- What personal data do you hold?
- Do you have special category data?
- Where is it from and where is it sent?
- Why is it processed? (For what purpose?)
- How is the processing lawful?
- Which of the conditions is met?

OFFICE OF THE INFORMATION COMMISSIONER

Office of the Information Commissioner
Brunel House
Old Street
St Helier
Jersey JE2 3RG
Email: enquiries@dataci.org
Telephone: +44 (0)1534 716530

Individuals Rights

GDPR significantly enhances and extends rights for individuals. This includes:

- Access to data (no fee required)
- Rectification of data
- Erasure of data ('right to be forgotten')
- Data portability
- Transparency

Action Required

- Review your privacy notices to ensure you provide individuals with all the necessary information about how their data are to be processed and what their rights are.
- You will need to put policies and procedures in place for the handling of requests for erasure and portability.

Consent

Where consent is relied upon, the GDPR will require it to be demonstrated by the data controller and involve clear, affirmative action. It must be clearly distinguishable, freely given and must be as easy to withdraw as it is to give. Where children's* data are processed on the internet, parental consent will be required. *(*the legal definition of a child will be determined at law drafting stage with the upper age limit required to be within the range of 13-16 years.)*

Action Required

- Review how you obtain consent and ensure you provide individuals with the information they are entitled to at the point of collection.
- If you are processing data relating to children, be aware that there will be additional requirements.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey GY1 2LQ
Email: enquiries@dataci.org
Telephone: +44 (0)1481 742074