THE OFFICE OF THE
Data Protection Authority

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the **Law**")

Carrying out a Data Audit

To ensure required levels of data protection compliance, you need to understand exactly what processing of personal data you are undertaking. A first step in establishing such an understanding at organisational level will require a comprehensive review and documentation of data for which you are controller and therefore have legal responsibility.

The documentation of a data audit will also assist you when it comes to demonstrating a proactive approach to your statutory obligations as well as future reporting requirements to the Office of the Data Protection Commissioner (ODPC).

This guidance document sets out suggested key steps that you may find helpful when conducting a data audit. You will need to tailor the questions and general approach based on your own particular circumstances.

Stage 1 - Planning the Data Audit

- Identify the sponsor. Ensure senior ownership.
- Identify who will be responsible for and lead the data audit

- Identify all other key personnel that need to be involved
- Agree access to relevant personnel, departments, systems and documents
- Agree the time personnel will be required to give to the audit
- Plan and document how the audit will be carried out

Stage 2 - Identify the Personal Data and How It is Processed

Key questions

- What personal data do we have?
- How did we get that personal data?
- What do we use the personal data for?
- What have we told individuals about what we will do with their personal data?
- Do we disclose our personal data to any other organisations?
- Where is that personal data located/stored/backed up/archived?
- How long is personal data held?
- Who has access to our data and for what purpose?
- How do they access our personal data?
- Do we use data processors who handle our personal data on our behalf?
- Is personal data transferred outside the Bailiwick of Guernsey and the EEA?

You know your organisation better than anyone so ensure you include questions that are relevant and specific to your own processing

- Create all data inventory documentation (e.g. questionnaires)
- Collect all necessary personal data and compile detailed inventory
- Identify any processing of **special category data**

Stage 3 -Assess Processing and Compliance

- Identify and document the lawful processing condition for all data sets you have identified
- Identify and document all locations of your personal data and measures to safeguard any transfers outside the Bailiwick of Guernsey and the EEA

- Identify and document how such personal data are processed including security measures, access controls etc.
- Identify and document all those (personnel and third parties) with access rights to your personal data
- Refer to ODPC guidance and the Law to identify areas of compliance and areas of non-compliance

Stage 4 - Report, Recommend and Make Changes

- Produce your audit report
- Flag areas that need further input – either because more information is needed or because there are elements of compliance that need review
- Make recommendations
- Secure approval of the report findings from the audit sponsor and communicate findings to senior management team/board
- Identify who is responsible for implementation
- Produce an action list and assign actions to relevant staff
- Ensure timely review of progress

Don't forget

- Review all third party contracts. The Law requires certain specific elements to be included in controller/processor agreements
- Review employee contractual and non-contractual documentation. Your staff need to understand the important role they play in ensuring compliance. Failing to ensure that areas such as staff training, contracts and handbooks are sufficient is likely to expose you to unnecessary and preventable risk
- Document the audit in a form that will assist in the event of any enquiry from the ODPC
- Retain the audit report and diarise regular reviews to ensure it is kept up to date