DATA PROTECTION COMPLIANCE AUDIT

Key findings from a Virtual Compliance Audit 2024-2025

Who we audited

Virtual audits were undertaken on a health service sector which processes significant volumes of special category personal data.

This sector of controllers was chosen for audit because we identified their processing activity as being in key risk areas for the processing of personal data, including the most sensitive information (special category information) relating to both adults and children. We have responded to several Self-Reported Data Breaches (SRDBs) and Enquiries concerning processing of personal information and technical and operational security.

Whilst the identities of the controllers will not be publicised, the key findings summarised here are taken from this audit and which we consider will be instructive to other controllers.

What our audit focused on

One of the functions of the Jersey Data Protection Authority [1] is to administer and enforce compliance with both Data Protection (Jersey) Law 2018 (the **DPJL 2018**) and the Data Protection Authority (Jersey) Law 2018 (the **DPAJL 2018**).

Our virtual audits were conducted as per our audit process. Our questions assessed the risk of non-compliance with reference to identified broad risk areas i.e. those areas where we believe that the absence of appropriate arrangements in these areas threatens the organisation's ability to meet its data protection obligations.

The scope of the audit focused on the risk of non-compliance with applicable data protection principles, with specific reference to 7 key areas:

1. **Data Protection Governance**
   Focus area: The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPJL 2018 compliance are in place.

   Risk: Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the DPJL 2018 resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

[1] See Article 11(1) of the DPAJL 2018

DATA PROTECTION COMPLIANCE AUDIT

2. **Training and awareness**
   Focus area: The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

   Risk: If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the DPJL 2018 resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

3. **Records management**
   Focus area: The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention, and destruction of personal data records.

   Risk: In the absence of appropriate records management processes, there is a risk that records may not be processed in compliance with the DPJL 2018 resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

4. **Security of personal data**
   Focus area: The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

   Risk: Without robust controls to ensure that personal data records are held securely in compliance with the DPJL 2018, there is a risk that they may be lost or used inappropriately, resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

5. **Data subject requests**
   Focus area: The procedures in operation for recognising and responding to individuals' requests for e.g., access to, rectification or erasure of their personal data.

   Risk: Without appropriate procedures there is a risk that personal data is not processed in accordance with the rights of the individual and in breach of Art.8(f) of the DPJL 2018. This may result in damage and/or distress for the individual, and reputational damage for the organisation as a consequence of

this and any regulatory action.

6. **Data sharing**
   Focus area: The design and operation of controls to ensure the sharing of personal data complies with the principles of the DPJL 2018 (including in respect of sharing of data between controllers, and international transfers).

   Risk: The failure to design and operate appropriate data sharing controls is likely to contravene the principles of the DPJL 2018, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.

7. **Risk assessment including Data Protection Impact Assessments**
   Focus area: The procedures in place demonstrate an effective risk assessment/DPIA process for use throughout the development and implementation of a project, in order to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

   Risk: Without effective processes in place to facilitate "privacy by design", there is the risk that the privacy implications of projects and resulting potential areas of non-compliance with the DPJL 2018 will not be identified at an early stage.

This may result in regulatory action, reputational damage to the organisation and damage or distress to the individuals who are the subject of the data.

What we found

We consider that it is important to highlight areas of good practice in industry, as well as areas for improvement and to explain what remedial action was required, and why.

Areas of good practice

The main areas of good practice were in relation to understanding and implementing the use of lawful bases, storage limitation, relevant retention schedules and the security of data subjects' information which included the use of appropriate data management systems.

DATA PROTECTION COMPLIANCE AUDIT

1. Lawful bases

There was good evidence of the audited entities demonstrating the correct interpretation and application lawful bases, as set out by the DPJL 2018, when collecting and processing personal information. It was particularly reassuring to note that the controllers were only relying on consent when appropriate and relevant to do so. This particular health sector leans on consent for much of its processing activities. It was clear that the entities have good knowledge of the various lawful bases and appropriate decisions are being made when sharing information both internally and externally.

2. Storage limitation and retention

The audited entities demonstrated confident control surrounding storage limitation and were able to evidence how long various types of data is retained and the reasons why. This was evidenced by the retention schedules supplied to the Authority during the audit process.

3. Information security and data management systems

The entities audited evidenced good knowledge regarding data security and the importance of keeping information secure, particularly as this industry processes high volumes of special category data. It is clear that the protection of data subjects' personal information is a priority and taken seriously. The entities generally deploy sector specific software platforms, common amongst them. The use of this similar data management system helps to foster a consistent approach to the secure processing of personal data under the DPJL 2018.

Areas for improvement

Overall, of the areas for improvement, we found that there was a lack of (bespoke) data protection training, data protection policies and procedures, and in some cases a lack of awareness and understanding regarding data sharing. Engagement with this sector was sporadic and although initial communications were positively received, entities appeared reticent to complete the virtual audits without reassurance from the Authority.

1. Staff Training

Whilst most of the entities provided training to staff, it was highlighted that it was of a generic nature, with entities using the same broad non-role specific training programme. The Authority strongly advised the entities to tailor data protection training to the needs and requirements of each entity and their specific job roles. A more bespoke training approach should be adopted.

DATA PROTECTION COMPLIANCE AUDIT

2. Data Protection Policies and Procedures

Although some entities had the relevant data protection Policies and Procedures in place, there were areas for improvements to be made, for example, ensuring the entities' Privacy Policies refers to the correct law (DPJL 2018) as opposed to General Data Protection Regulations (GDPR). Some of the Retention Policies also referred to UK regulations, so entities were advised to consider that relevant Jersey regulations should be referenced. It was also noted that some policies also made reference to the previous Data Protection (Jersey) Law **2005** instead of the current DPJL 2018 law.

There were a number of entities which did not have appropriate data protection policies and procedures in place, such as a privacy policy outlining data subject rights, an internal breach log to record any data breaches and a retention schedule. They were tasked with completing these to a satisfactory standard.

3. Data Sharing

The audit highlighted in some entities there was confusion and lack of awareness surrounding data sharing. This sector, by nature, is responsible for sharing a large quantity of personal data and in particular special category data. The audit feedback highlighted the lack of understanding in relation to data sharing protocols and procedures. Relevant data sharing agreements must be reviewed in order to avoid the risk of damage or distress for individuals, regulatory action and reputational damage to the organisation.

Why this is important?

Organisations must have in place robust controls, policies, procedures and provide appropriate training to ensure the safety of individuals' data and mitigate potential risks.

Personal information, if mishandled, can lead to significant consequences for data subjects. For example, the processing and/or sharing of incorrect information can influence life changing decisions, whilst loss of information can lead to identity theft, financial fraud, or privacy breaches. With proper controls and policies in place however, organisations can manage access to sensitive data, prevent unauthorised use, and respond effectively to security breaches. Ultimately, these measures not only protect personal information but also build trust between organisations and the individuals they interact with.

Best Practice

Data Protection Training

Training should be specific and tailored (insofar as is possible) to the role carried out by the employee to ensure it is adequate and equips the employee with the skills they need to carry out their role and assist the controller in upholding its data protection obligations.

Where relevant, training should be provided to all new employees prior to being given access to systems and areas of the organisation's personal information and on a frequent basis (at least annually) thereafter and include:

a. Reference to local legislation and relevant requirements.
b. Information regarding what special category personal data is and how it should be handled.
c. Sharing personal data.
d. Retention and safe destruction of personal data.

Data Protection Policies and Procedures

Proportionate and effective policies and procedures to create a robust framework for handling personal data and implementing key measures to protect personal data must be in place and effectively communicated. Organisations should ensure that staff are aware of the policies and procedures and check that such are actually being adhered to and followed, in practice.

Confidentiality

To support confidentiality, where required, office layout and the use of privacy screens should be evaluated. Confidentiality and office layout extends to reception areas and building access depending on the mix of visitors and staff etc. The regular training should also cover confidentiality.

Next Steps

The organisations audited received direct feedback from the Authority's audit team where areas for improvement were identified and proposed. A number of entities were required to respond directly to us to confirm remedial action had taken place. We are continuing to work alongside one entity.

We want every organisation to feel confident in their understanding of their data protection obligations. It is critical that where improvements are to be made, these are effective and sustainable for the broader Jersey community.