JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

DATA PROTECTION COMPLIANCE AUDIT

Key findings from a Virtual Compliance Audit 2023/4

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 received complaints regarding this sector, concerning personal information 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 demonstrating 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 area for improvement and to explain what remedial action was required, and why.

Areas of good practice

There was good engagement from this sector, timely responses, and participants appear to be committed to getting both the responses and data protection practices correct which is appreciated. Overall, it was good to note the extent of documentation in place which is indicative of this sector's overall understanding of data protection and its importance.

In relation to Data Protection policies and procedures, we found that all of the entities had a Privacy Policy, retention schedule, acceptable use policy and a

DATA PROTECTION COMPLIANCE AUDIT

breach log in place and they were all of a satisfactory standard, requiring only minor alterations.

We also found that all entities had a Subject Access Request (SAR) process in place and a copy of the policy was provided by all entities. Again, they were all of an adequate standard and some general advice and guidance was provided for potential improvements.

All of the entities provide Data Protection induction training when staff members join, and the majority of them provided training at the recommended, regular intervals, i.e. every 6-12 months. We were also provided with evidence of the training, which is rolled out to staff members however, some advice and guidance was provided in order to make improvements.

When the Authority reached back out to the entities upon reviewing their initial Audit responses, all of them embraced the feedback, advice and guidance and we were advised that improvements were going to be put in place to ensure and maintain high standards of Data Protection compliance. It was also agreed that they would engage further with the Authority after a period of time of putting improvements in to place.

We also found that the software systems in use had audit functions and appropriate, role-specific access controls enabled to manage conflicts and ensure access to information was limited to those who need it.

In addition, we identified strengths in the controller's breach management procedures, with the majority of employees stating they were able to identify a data protection breach and felt comfortable reporting breaches to the relevant person/department; they felt supported and did not fear repercussions should they have to report issues caused by their own human error.

Areas for improvement

Overall, of the areas for improvement we found that many related to the understanding reporting thresholds, definitions, retention matters, plus administering data subject individual rights, staff awareness of policies, correct skills and training.

1. <u>Restricting Access.</u>

   It was noted that some of those audited entities did not limit access to the most sensitive of information to those only who need it. Restricted access would help to mitigate the risks associated with living in a small community.

DATA PROTECTION COMPLIANCE AUDIT

2. Staff Training.
   All the audited entities provided both induction and interval training in relation to data protection. One entity was advised to increase the frequency of training delivered to staff, to a minimum of twice per annum given the risk of the data they process.

3. Data Protection Policies and Procedures
   Although all entities had the relevant Policies and Procedures in place, there were areas for improvements to be made, for example, ensuring the Privacy Policy refers to the correct law (DPJL 2018) as opposed to GDPR. There was also some confusion surrounding data controllers and data processors. Some of the Privacy Policies indicated that staff members were regarded as processors and certain individuals in the business were named as controllers as opposed to the actual business name. Some of the Retention Policies also referred to UK regulations, so entities were advised to consider whether Jersey regulations should also be applicable.

4. Communication Channels
   It was established that a large number of entities used various social media platforms when communicating to internal staff and external data subjects, but it was recognised by the Authority that the communications were often too identifiable and therefore posed a security risk. Entities were advised to review their areas of communication and ensure they have a clear policy in place to reflect which platforms can and can't be used, how, and what for.

Why this is important

Organisations must have in place robust controls, policies, procedures, technology, 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.

DATA PROTECTION COMPLIANCE AUDIT

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 yearly) 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 audit team where areas for improvement were identified and proposed. Only one entity was required to respond directly to us to confirm remedial action had taken place.

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 organisations.