DATA PROTECTION COMPLIANCE AUDIT

Key findings from a Full Compliance Audit
2023/4

Who we audited

A recent full audit focused on one important local Public Sector data controller which processes significant volumes of personal data.

This controller 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. Historically, we had also received complaints regarding this organisation, frequently relating to issues about confidentiality and data sharing often as a result of a lack of staff training on data protection.

Whilst the identity of the controller 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

Our face-to-face audit was conducted as per our audit process, and the scope of the audit was agreed with the controller, focusing on the risk of non-compliance with applicable data protection principles, with specific reference to two key areas:

1. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities; and

2. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

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

We were pleased to note that there were areas of good practice regarding the controller's technical security measures such as devices having MFA enabled and protected with complex password requirements. In addition, the controller did not permit the use of personal devices to carry out any work-related activities and this was set out in certain of the controller's policies, with evidence provided that such stipulations were actually adhered to by the

controller's staff (i.e. working practices actually reflected the intention and instructions of the controller).

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 staff awareness of policies, correct skills and training and we also found that the audit participants were not always briefed, prepared and organised to participate in the audit to allow the process to be conducted effectively in terms of time and contributions.

A number of deficiencies in systems and controls were identified, however, which if left unremedied, would have likely resulted in further enforcement activities taking place, as such will expose the controller to risk in terms of the potential exposure of the personal information handled by them (which could, in turn, impact on affected data subjects).

1. Data Protection Training
   It was noted that the controller's training on data protection lacked specificity and it had adopted a one size fits all approach, irrespective of the employee's position within the organisation and the type of information they had access to.

2. Data Protection Policies and Procedures
   Employees were unaware and unfamiliar with certain organisational policies and procedures. This included policies in relation to data security, the retention of personal data and safe destruction.

3. Data Sharing
   Employees were not confident to know when it was permissible/desirable to share or not share personal data with a third party. Employees were unaware of any data sharing agreements in place between the controller and external agencies to enable and support the sharing of personal data with third parties.

   In addition, employees were often unclear which lawful basis was being relied upon to share personal data and often reverted to consent which could cause complications if consent was not provided.

4. Confidentiality
   The office 'set-up' was generally open plan with a lack of confidential spaces for employees to discuss matters without the risk of others overhearing and being privy to information they otherwise had no lawful basis to be aware of.

5. Messaging and virtual meeting applications
   Concerns were raised regarding computer system notifications (e.g. email alerts) becoming visible to third parties where an employee's screen was visible, whether during physical or online shared screen meetings. This creates the risk of personal data being exposed to unrelated third parties.

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 and use, and respond effectively to security breaches. Implementing technology (like encryption and secure databases) fortifies the defence against cyber threats. Moreover, regular training for employees on data handling best practices is essential to maintain a vigilant and knowledgeable workforce, reducing the likelihood of human error that could compromise data security. 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

Instead of basic tick box, generic, training, the 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 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 hat such are actually being adhered to and followed, in practice.

Personal Data Sharing

Where Employees are required to share information as part of their role, they must be clear which lawful basis they are relying upon to share personal data. Lawful bases for sharing must be identified before any sharing takes place and employees must know when they can share information and know how to document any decisions made.

Organisations must also ensure that relevant data sharing agreements are in place between parties where needed before personal data is shared and where appropriate, ensure employees are aware of such agreements.

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.

Messaging and virtual meeting applications

- Organisations should create guidelines for employees recommending that all irrelevant apps are closed before meetings (either physical or virtual) where the screen might be visible to other parties. Alternatively, consider providing technical support around notification management to provide employees with the ability to temporarily turn off notifications during meetings.

- Organisations should clearly document any decision regarding the use of messaging platforms to discuss clients or other individuals in a work capacity. A policy or guidelines should be created setting out the organisation's stance on the use of messaging platforms (to include which platforms can/cannot be used) and circulated to all

DATA PROTECTION COMPLIANCE AUDIT

employees to ensure they are all aware and there is consistent approach.

- If considered it is acceptable to use such messaging platforms to discuss clients and other individuals, it is important that employees are made aware that conversations will be discoverable and may be disclosed upon receipt of a subject access request. The personnel responsible for responding to any such requests should ensure that all relevant messaging platforms are included in the search following receipt of a subject access request.

Next Steps

The organisation audited received direct feedback from the audit team where areas for improvement were identified, the organisation was required to make changes as directed and in accordance with our stipulated timeframe.

We want every organisation to feel confident in their understanding of their data protection requirements and that where improvements have been made, that these are effective and sustainable for that organisation noting its size, the resources available to it but appropriate to the risks associated with the information it processes.