Department for Education (DfE)

Data protection audit report

February 2020

Information Commissioner's Office

Executive Summary

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices.

The Commissioner's Enforcement team ran a broad range investigation in 2019 following complaints from DefendDigitalMe and Liberty and their concerns around the National Pupil Database (NPD). The ICO met with key senior level data protection professionals at the DfE's offices in London in November 2019 where the possibilities of a consensual audit were discussed. However, due to the risks associated with the volume and types of personal data processed within the NPD as well as the ages of the data subjects involved, the Commissioner decided, in line with her own Regulatory Action Policy, to undertake a compulsory audit using her powers under section 146 of the DPA18. The Commissioner determined this approach would provide a comprehensive review of DfE data protection practices, governance and other key control measures supporting the NPD and internally held databases, using the framework of scope areas of audit as listed below. This would allow the Commissioner to identify any risk associated with the data processed and implications to the individual rights of over 21 million data subjects.

An Assessment Notice was issued to the Department for Education (DfE) on 19 December 2019. The audit field work was undertaken at DfE Offices in London, Coventry, and Sheffield between 24 February and 4 March.

The DfE agreed to extend the scope of the audit to include the sharing of data contained within the Learning Records Service (LRS) database to assist an ICO investigation following a reported data breach.

The scope of the audit covered the following key control areas:

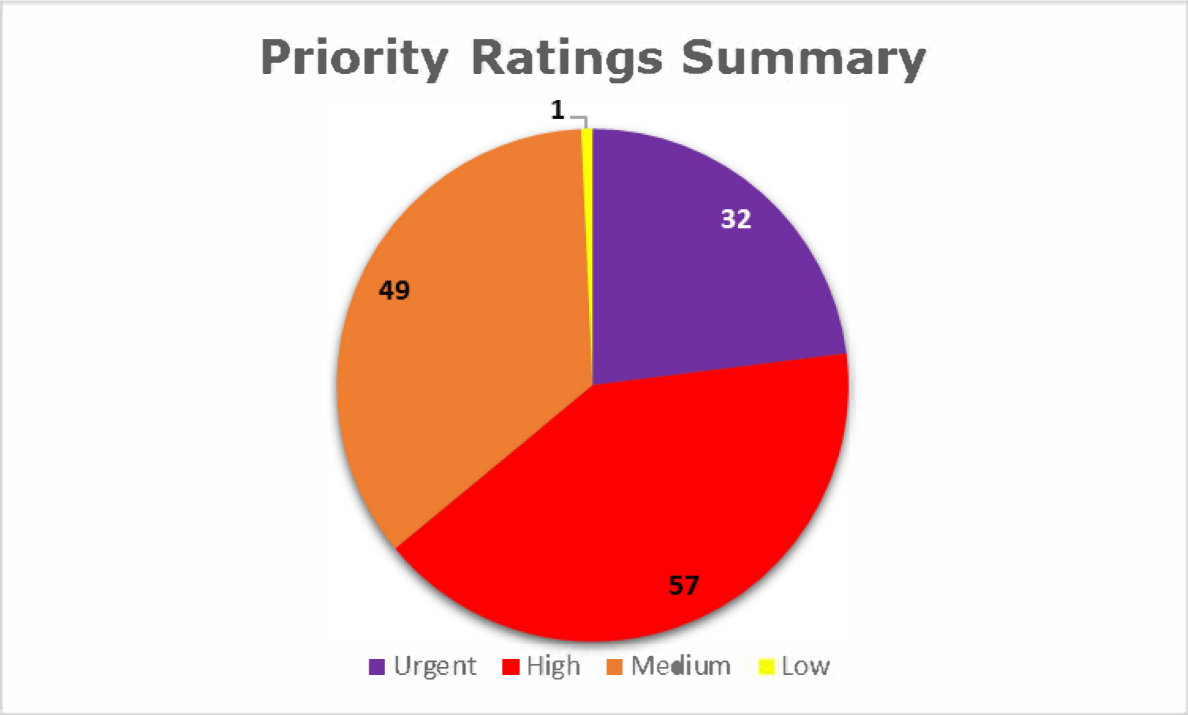
- Governance & Accountability
- Individual Rights
- Training & Awareness
- Information Risk
- Data Sharing
- Records Management
- Information Security

The purpose of the audit was to provide the Information Commissioner with an assurance of the extent to which DfE, within the scope of the audit, is complying with data protection legislation.

Priority of recommendations summary

Where opportunities for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the DfE in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The DfE's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

A summary of the ratings assigned within this report is shown below.



Urgent priority recommendations are intended to address risks which represent clear and immediate risks to the DfE's ability to comply with the requirements of data protection legislation.

Areas for Improvement

- There is no formal proactive oversight of any function of information governance, including data protection, records management, risk management, data sharing and information security within the DfE which along with a lack of formal documentation means the DfE cannot demonstrate accountability to the GDPR. Although the Data Directorate have been assigned overall responsibility for compliance actual operational responsibility is fragmented throughout all groups, directorates, divisions and teams which implement policy services and projects involving personal data. Limited reporting lines, monitoring activity and reporting means there is no central oversight of data processing activities. As a result there are no controls in

place to provide assurance that all personal data processing activities are carried out in line with legislative requirements.

- Internal cultural barriers and attitudes are preventing the DfE from implementing an effective system of information governance, which properly considers the rights and freedoms of data subjects against their own requirements for processing personal data to ensure data is processed in line with the principles of the GDPR.

- The organisational structure of the DfE means the role of the Data Protection Officer (DPO) is not meeting all the requirements of Article 37-39 of the GDPR. The legislative requirement for the DPO to inform and advise the controller is currently fulfilled by Privacy and Information Rights Advisory Service (PIRAS) who, only offering an advisory service and with no formal links to the DPO, have no accountability to the GDPR.

- There is no policy framework or document control in place which means that key policies such as an Information Governance Framework or Data Protection Policy have not been created. Policies that are in existence demonstrate no version control and are not subject to any formal review procedures meaning that many are out of date and ineffective. There is no governance over the creation review and approval of policies meaning there is no consistency in style, approach or content used across the range of directorates responsible for producing them.

- There is no clear picture of what data is held by the DfE and as a result there is no Record of Processing Activity (ROPA) in place which is a direct breach of Article 30 of the GDPR. Without a ROPA it is difficult for the DfE to fulfil their other obligations such as privacy information, retention and security arrangements. The requirement for a ROPA has been documented for over a year in audit reports and meeting minutes, however little progress has been made to address this.

- The DfE are not providing sufficient privacy information to data subjects as required by Articles 12, 13 and 14 of the GDPR. There is also some confusion within the DfE and its Executive Agencies about when they are a controller, joint controller or processor and whether as a controller this is at the point of collection or as a recipient of personal data. Equally there is no certainty whether organisations who receive data from the DfE are acting as controllers or processors on their behalf. As a result, there is no clarity as to what information is required to be provided. The DfE are reliant on third parties to provide privacy information on their behalf however, this often results in insufficient information being provided and in some cases none at all which means that the DfE are not fulfilling the first principle of the GDPR, outlined in Article 5(1)(a), that data shall be processed lawfully, fairly and in a transparent manner.

- The DfE are providing very limited training to staff about information governance, data protection, records management, risk management, data sharing, information security, individual rights and in some cases there is no assurance that staff are receiving any training whatsoever. Given the volume and categories of personal data being processed the lack of awareness amongst staff presents a high risk that data will not be processed in a compliant manner and could result in multiple data breaches or further breaches of legislation. In addition, there is a reliance on staff to become self-aware of policies and procedures without follow up or acknowledgement which means there is no assurance that they have been read or understood.

- The Knowledge and Information Management Team (KIM) have no active involvement with the NPD which means there has been no expert involvement to develop appropriate procedures for the creation storage and retention of records which include formal documentation of what information is added to, or not added to, the NPD from any given information collection, weeding of records and retention and disposal of NPD information including appropriate documentation.

- Information risks are not managed in an informed or consistent manner throughout the DfE or in line with the Risk Management Framework. Information assets are not assessed with sufficient frequency to ensure that the process is effective and resulting risks are not recorded with sufficient granularity or detail on the Information Risk Log to enable meaningful control and monitoring. Not all information risks are recorded and where they are, they do not always identify actual risks or control measures.

- Data protection impact assessments (DPIAs) are not being carried out at a stage of the project early enough to influence the outcome and in some cases prior to processing beginning altogether. Some processing which should have been subject to a DPIA is being carried out without any DPIA having been completed. The Privacy Assurance Team (PAT) are risk assessing projects they aren't fully briefed on, resulting in high level content with no detailed risk assessment of the specifics of the processing activities, and the mitigation actions identified do not often have appropriate effects on the residual risk scores. The assignment of lawful basis in DPIAs is also high level and does not include a justification for the designated lawful basis or details of how it applies to each specific processing activity.

- The Commercial department do not have appropriate controls in place to protect personal data being processed on behalf of the DfE by data processors. Which means there is no assurance that it is being processed in line with statutory requirements particularly where processing contracts are of low enough value to not be subject to formal procurement procedures. Processor and third party due diligence does not always consider whether appropriate organisational and security measures are in place to provide the DfE with assurance that personal data will be processed in line with statutory requirements.

- The Data Sharing Approvals Panel (DSAP) official remit is to govern all of DfE's external, individual level data sharing. Whilst DSAP is the official gateway for shares, not all sharing decisions throughout the DfE and its executives agencies are considered by DSAP so there is limited oversight and consistency around how data is shared externally.

- The two formalised assessments used by both DSAP of a data request application and the caseworkers who represent an application through to DSAP are based on the five safes and the four principles of sharing data. Consistent assessments to granularly inform the purpose, legality and risks of the application are not formally carried out and there is no requirement for a DPIA to be carried out for all sharing applications. As a result there is no formal assessment of applications for data protection compliance.

- There is an over reliance on using public task as the lawful basis for sharing which is not always appropriate and supported by identified legislation. Legitimate interest has also been used as a lawful basis in some applications however there is limited understanding of the requirements of legitimate interest and to assess the application and legalities of it prior to sharing taking place how it should be applied to ensure the use of this lawful basis is appropriate and considers the requirements set out in Article 6(1)(f) of the GDPR.

- In 400 applications, only approximately 12 were rejected due to an approach which is designed to find a legal gateway to 'fit' the application rather than an assessment of the application against a set of robust measures designed to provide assurance and accountability that the sharing is lawful in line with statutory requirements.