Annex: Data Protection Officer's Annual Report 2020/21

Agenda Item 6 Paper Ref 03d

1. Summary

In exercising its functions, Social Work England processes the personal data of members of the public, social workers, education and training providers, members of staff, and third parties such as businesses that provide services under contract. This report summarises the organisation's key activities in relation to data protection and compliance with data protection law. It pertains to the period from 1 April 2020 to 31 March 2021.

Social Work England is registered as a data controller with the Information Commissioner's Office. Its ICO registration number is ZA498223.

2. Activities and approach

This particular edition of the Data Protection Officer's report is the first to review a full year of Social Work England's operations. Operations were largely delivered remotely, due to the legal restrictions placed on movement and contact in response to the Covid-19 pandemic, and at a time when the transition period for the UK's exit from the European Union came to an end. The organisation's data protection-related activities included, amongst other things:

- Providing training and support throughout the organisation
- Responding to and learning from data incidents
- Establishing and reviewing the provisions in contracts with third parties
- Cataloguing information assets and data processing activities
- Establishing reporting governance to the Board, the Audit, Risk and Assurance Committee and the Executive Leadership Team
- Introducing data sensitivity and retention labelling in Office 365
- Responding to legal developments such as Schrems II and the end of the EU exit transition period

3. Individual data rights requests

Social Work England received 258 individual data rights requests for which a response was due within the reporting period. 203 of these were data subject access requests (DSARs), and the remainder comprised other requests such as for the erasure of personal data that we hold, or requests from the police for information. All except one of these requests were responded to within the statutory timeframe, which is usually no later than one month from the date of receipt of the request. The one request which was not responded to within the statutory timeframe was a DSAR sent to the general enquiries email address in February

2021; this was not identified as a DSAR until the requestor contacted us again in May 2021 to pursue a response.

The number of individual data rights requests decreased at the beginning of the first Covid-19 'lockdown' in the UK, with just 27 requests being received in the four-month period between 1 April and 31 July. The number of requests has increased substantially since that time, with a monthly high of 53 requests received in March 2021.

4. Data incidents

100 data incidents were reported to, and investigated by, the organisation.

This figure includes 54 data breaches, 30 'near misses' and 16 non-Social Work England data incidents.[1]

Social Work England has adopted an internal response system for data incidents, based on the degree of risk to the rights and freedoms of the data subject(s) and the number of data subjects affected. None of the data incidents have been assessed as being *likely* to result in a risk to those *rights and freedoms*, for example, damage to reputation, or an adverse effect on private and family life.

The types of incidents have involved, for example, emails being sent to the wrong email address, and documents containing details for the wrong person being attached to emails.

The Information Governance Steering Group[2] (IGSG) reviews data incidents on a regular basis, and the Audit, Risk and Assurance Committee is also routinely briefed on significant incidents and incident trends generally. Organisational changes designed to reduce the risk of repetition, such as the provision of training or IT measures such as data classification and warnings where an email address comes from an external recipient, have been implemented in response.

No incidents have been deemed to meet the threshold of risk which would require them to be reported to the ICO.

5. Training

Employees and board members have been asked to complete a GDPR e-learning module. This was completed by 97.5% of employees (since May 2020), 97.8% of Partners (since January 2020) and 100% of board members (since the inception of Social Work England).

---

[1] A near miss is defined for these purposes as a data incident that had the potential to cause or amount to a data breach but did not do so; there was no access to personal data outside of the organisation. 'Non-Social Work England data incidents' include, for example, where Social Work England has been sent personal data in error, or a member of staff has found personal data left on the premises. Such incidents are logged so that, if necessary, the organisation can demonstrate how it dealt with the situation.

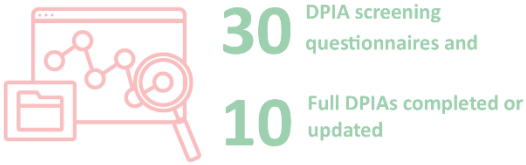
[2] The IGSG is a committee accountable to the Executive Leadership Team. It comprises senior stakeholders with accountability for information governance. Its purpose is to support and drive the broader information governance agenda and provide Social Work England's Executive and Board with the assurance that robust information governance is in place within the organisation.

6. Data Protection Impact Assessments (DPIAs)

A DPIA screening questionnaire is used to help identify the need for a full DPIA, which involves more extensive consideration of the data protection risks and how these can be mitigated.

30 DPIA screening questionnaires and 10 full DPIAs were completed or updated in the period up to 31 March 2021. The full DPIAs covered significant activities such as Social Work Week, the implementation of a new HR/finance/commercial system, and the review of the whistleblowing policy.

7. The year in numbers – at a glance



8. Areas of risk and looking to the future

The organisation has made good progress in developing the maturity of its information governance framework, as outlined above under 'Activities and Approach'.

Areas where further work is needed include:

- DPIA required on sending out hearings bundles
- Improvements to the information provided about cookies operating on the website, and the functionality of the cookie banner (to ensure that it is as easy to withdraw consent as it is to give it)

- Technical measures to give effect to data retention periods in other internal systems beyond Office 365, to ensure that data is kept where it is needed, but for no longer than necessary
- Migration to a new survey tool to improve internal access control to survey responses
- Reviewing and updating records of personal data processing activities
- Considering our approach to seeking and recording a commitment to confidentiality from existing staff. New staff (since April 2020) have a contractual duty of confidentiality.
- The establishment of new and the review of existing data sharing agreements with organisations with which we share data, or which share data with us, in order to facilitate the exercise of our regulatory functions.
- Development of an internal policy regarding the security measures taken when sending email attachments
- Implementing mid-contract and end-of-contract checks on data protection compliance/performance where we contract with third parties, and a review of the legal provisions in contracts where data processing takes place outside of the UK
- Updates to the website privacy notice, including more information about data retention
- Changing the system used to capture and record individual rights requests, so that it is done in the case management system rather than recording the requests on a spreadsheet

The likelihood and impact of these risks to data subjects is monitored by Social Work England, and is limited by internal controls. The Executive Leadership Team is fully aware of these risks. All will be addressed and mitigated as part of a planned process for the 2021/22 financial year.

9. Final thoughts

The organisation continues to focus on protecting and upholding the rights and freedoms of the people whose personal data it holds. When things go wrong, it takes a "system" approach – focusing on the conditions under which people work, and building defences to reduce the risk of repetition or mitigate the effect, rather than blaming individuals, for example for some purported forgetfulness or lack of care. At the same time, it continues to support and emphasize both institutional and individual accountability and responsibility, to ensure a healthy and positive approach to the ownership and management of personal data. This culture is becoming embedded in the organisation as it proceeds into its second full year of operation.

Key activities during this reporting period, which further highlight the system approach, have included two projects to implement data sensitivity and retention labelling in Office 365. These have ensured that data classification and retention are not merely recorded in a policy document. There is no "pie in the sky" assumption of total compliance on the part of staff, but instead the policies are given practical effect. Classification and retention periods are applied by default, and the tools and training provided are designed to make it as easy as possible for staff to manage as part of routine working practices. In the case of sensitivity

labelling, the controls associated with the labels also help to reduce the risk of a data breach.

Following a busy and challenging year, there is more to do to address the identified risks, and some have persisted once identified. However, the board should be encouraged by the overall approach the organisation has taken to data protection during this period, and the culture that is developing to overcome challenges.

Gregory Lawton

Head of Data Protection and Information Governance

Data Protection Officer

Report finalised: 14 May 2021