DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to the Ministry of Justice (MOJ) in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain infringements of the UK GDPR.

The MOJ is the data controller for HMP [redacted]. [redacted] NHS Foundation Trust also provides healthcare services into the prison. As a result some of the confidential waste held by the prison contained confidential medical records.

A security incident occurred on 26 February 2022. 14 bags of confidential waste were found in an unsecured holding area in the prison which both prisoners and staff had access to. A shredder would usually collect the confidential waste. On this occasion the shredder lorry did not collect the bags within the allotted time leaving them unsecured, for a period of 18 days in total.

In addition to being in an unsecured location, some of the bags had not been sealed or shredded correctly and contained information relating to both prison staff and prisoners. This included medical data, security vetting details and a [redacted] Report [redacted].

During this period we are aware that 44 individuals potentially viewed the information contained in the confidential waste bags. [redacted] prisoners were identified as having removed information.

Despite evidence of certain staff challenging prisoners who were seen to read papers contained in the bags, the staff did not subsequently report that confidential waste was being stored in the unsecure area. It is established that there were no pre-agreed areas for staff to leave confidential waste securely at HMP [redacted].

The prison does not hold accurate data on the number of staff that had completed data protection training at the time of the incident.

The reprimand

The Commissioner has decided to issue a reprimand to the MOJ in respect of the following infringements of the UK GDPR:

- **Article 5(1)(f) - Security and Article 32(1)(d) & (2) which state:**

Article 5(1)(f)

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 32(1)

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 32(2)

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The reasons for the Commissioner's findings are set out below.

Article 5(1)(f) and Article 32(1)(d) & (2)

The MOJ had not implemented the appropriate technical and organisational measures to ensure the security of the personal data in this case. As a consequence, data was left unsecured in an accessible area to

other prisoners and prison staff.

Lack of robust policies

Whilst is it noted that the MOJ had policies in operation that clearly emphasise the need to securely shred records, there was no specific instructions provided to prison staff in relation to the designated storage areas for confidential waste prior to its disposal. Clarity in this regard would likely have prevented the waste bags from being left in an unsecure area by prison staff.

The established processes for holding and disposing of confidential waste were not sufficient at the time of the incident.

The guidance in relation to [redacted] reports relates to the prison's general use of its [redacted] System, and does not make specific reference to the appropriate handling of [redacted]. The prison should have established more granular instructions for staff for the handling or disposing of [redacted] This would have mitigated the risks of inappropriate disclosure.

Whilst data breach reporting and guidance documents were in place at the time of the incident, the ICO has been provided with minimal evidence to demonstrate that established data incident reporting requirements, were sufficiently reinforced to prison staff at appropriate intervals. Staff lacked understanding of the risks and need to report the data breach.

The prison staff involved in placing the confidential waste in the unsecure area were found to have a lack of awareness of processes for handling sensitive and confidential waste. Furthermore, staff were not aware of the need to shred information prior to its disposal and did not understand the risk of using prisoners to move confidential waste.

Whilst it is established that data protection training is in place, there were no robust measures in place to ensure that staff were completing the mandatory training.

The completion of such training by prison staff is crucial to embedding a culture of risk awareness and confidence in identifying potential data breaches. Had this training been undertaken in line with established

requirements, staff would have been more likely to recognise their responsibilities in appropriately securing the confidential waste and/or reporting the data breach incident at an earlier stage.

Severity of breach

It has been established that up to 44 individuals viewed the information contained in the confidential waste bags. As a result the risks to individuals in the prison would be significant and include potential identification within the prison or outside in the wider community. There would also be a significant risk of intimidation by other prisoners. Outside of the individuals incarcerated, there is also the risk of unwarranted attention of family members if identified.

Mitigating factors

In the course of our investigation, we have noted that:

a) Once the breach was discovered, the waste bags were transferred to a secure location by a staff member within the prison.

b) The incident was reported to the prison's Information Security Team via email and senior staff and the [redacted] were also informed of the incident for oversight purposes. An internal investigation commenced.

c) The cells of the [redacted] prisoners initially identified as having accessed the waste bags were searched with no information found and relevant CCTV footage reviewed to identify other prisoners who had access to the data.

Remedial steps taken by the MOJ

The Commissioner has also considered and welcomes the remedial steps taken by the MOJ in light of this incident. In particular HMP [redacted] has implemented a new process to ensure all confidential waste is collected within the allocated time slot. Secure areas have now been identified for confidential waste and staff made aware of the new procedure. Sufficient shredders have now been brought on site, to ensure prior shredding of confidential waste can be completed.

Additionally, guidance will be issued to staff by HMP [redacted] for future [redacted] report disseminations. In particular, any disseminated [redacted] reports moving forward will contain instructions on appropriate handling and

disposal.

Decision to issue reprimand

Taking into account all the circumstances of this case including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to the MOJ in relation to the infringements of Articles 5(1)(f) and 32(1)(d) & (2) of the UK GDPR as set out above.

Further Action Recommended

The Commissioner recommends that the MOJ should take certain steps to ensure its compliance with UK GDPR. With particular reference to Articles 5(1)(f), 32(1)(d) and 32(2) of the UK GDPR, the following steps are recommended:

1) The MOJ should conduct a thorough review of all established data protection policies, procedures and guidance documents to ensure that these remain adequate for purpose and reference up to date legislation.

For example, it is noted that its Information Security Policy currently references the DPA 1998, its Information Security Policy Framework references GDPR rather than UK GDPR and its 'Records, Information Management and Retention Policy' has not been updated since 2018.

2) As part of this process, the MOJ could consider the creation of a separate data breach reporting policy and procedure for its staff (incorporating its incident reporting template) in place of its current inclusion in wider information security policies (ie to highlight the significance of the process).

3) Residual risks posed to affected individual(s) as a result of the disseminated and later exposed [redacted] reports should be tested in future to ensure these are sufficiently mitigated.

4) A data processing agreement or similar contract between the prison and the Trust should be formed, to outline any established controllership responsibilities surrounding the handling and eventual destruction of Trust data processed at the prison.

5) The MOJ should ensure that any further remedial actions outlined in its

correspondence to the ICO (particularly those related to staff training) are completed in a timely manner.

MOJ should provide the ICO with a progress update on the above recommendations in six months' time, ie by 27 October 2023.