DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to the Metropolitan Police Service (MPS) in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain alleged infringements of the DPA 2018.

The reprimand

The Commissioner has decided to issue a reprimand to MPS in respect of the following alleged infringements of the DPA 2018:

- Section 38(4) of Part 3 of the DPA 2018 which states: "all reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes."

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

It was of concern that MPS was unable to ensure that sensitive criminal records were not able to be uploaded correctly to the Police National Database (PND), or amended, or deleted and that this situation had been in place, unknown to MPS for some considerable time. The consequences of this failure cannot be measured but had the potential to cause significant damage.

Of particular concern was that, even though PND had been operational since 2011 MPS had not developed any automated system of checks to ensure that the vast number of criminal record files that were uploaded daily to PND were correctly loaded. In the response to enquiries, MPS described the system of checks at the time of the incident as "immature". This is concerning given the length of time that PND had been operational when the incident was discovered.

While it is accepted that an incident of this sort may not have been foreseen and that an automated checking system may not have been considered necessary, it does point to MPS not fully considering possible areas of system failure from the outset. Given the sensitive nature of the criminal record files involved some consideration of possible system failures would be expected. From the evidence presented this did not occur at any time since PND was instituted. In this matter MPS did not ensure the accuracy of the information it was in control of.

While it is also accepted that completing manual checks would have been extremely difficult given the volume of records involved, an automated system was able to be deployed as a remedial measure following the incident. This showed that that a reliable system of checks could have been deployed at any time, and would, in all likelihood have ensured that this incident did not occur.

Consideration has also been given to the fact that, while it is true that no records were lost and that information on Organised Crime Groups (OCG) would still be available on MPS systems, accurate information would not be available to partner police services or other agencies that use PND. It is of particular concern that partner agencies would not have been aware of updates to criminal records. This had the potential to cause significant issues for those agencies.

Law enforcement agencies may use PND to assess if a particular criminal or criminal group may be under the attention of a partner organisation. That accurate and up to date records would not be available would deny a partner knowledge which could conceivably have compromised an investigation. It is, therefore of particular concern as to how this incident affected partner agencies and what damage may have been caused as a result of accurate information not being available on PND.

It was of also of concern that MPS did not inform partner organisations of the incident until December 2020, more than six months after the discovery of the first issue. It is understood that MPS had to determine the scale and scope of the problem before it could inform partners fully. However, it would be expected that some warning would be given to ensure that partner agencies were aware of the potential deficiencies of the information provided by MPS for PND at that time.

Furthermore, while there has been no evidence presented of any actual damage caused as a result of the criminal records not being available, it cannot be stated, categorically that no damage was caused because of this incident. The fact is that it can never be known what actual damage has been caused as a result of these failings.

Mitigating factors

In the course of our investigation, we have noted that this case involved vast numbers of criminal records being added to PND for OCG daily, as well as a large number of record files being amended and deleted, as necessary. The volume of records meant that MPS had found it difficult to implement manual procedures to check the processes of uploading and amending.

It is understood that MPS's own criminal and intelligence records and systems were not affected and that all information could still be found via other MPS systems, though these systems may not have been available to other law enforcement agencies.

It is recognised that no records were actually lost and that there was no loss of any personal data as a result of the incident. However, the incident did lead to information not being available and not being correctly updated or deleted when required.

MPS has emphasized, and this has been noted, that these issues relate only to one of the databases that comprise PND. It is only files in the OCG database that have been affected. It has therefore not compromised the bulk of information that is available on PND to police services and other agencies that use PND.

Remedial steps taken by MPS

The Commissioner has also considered and welcomes the remedial steps taken by MPS in the light of this incident. In particular, it is understood that that all issues have now been addressed, and that enhanced monitoring frameworks have been implemented locally, and via support functions to prevent a recurrence of the issues in this incident. In addition, there will be ongoing oversight from the MPS Senior Responsible Officer, as well as MPS technical teams to ensure that any chance of a recurrence of this kind of incident is very much reduced.

Decision to issue a 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 MPS in relation to the infringements of section 38 of Part 3 of the DPA 2018 set out above.

Further Action Recommended

The Commissioner recommends that MPS should take certain steps to ensure its compliance with DPA 2018. With particular reference to section 38 of Part 3 of the DPA 2018, the following technical steps are recommended:

1. MPS should review how its codebase is managed. If GIT, or a similar version control system, is being used then there are steps that the ICO would expect would be taken. These include, protecting deployment code branches, ensuring code reviews take place before deployment, and training staff members in these practices. If a different system is being utilised to manage the

codebase, other than GIT, then the ICO expects equivalent measures to be in place.

2. This incident would have likely been mitigated if there had been proper protection of deployment code branches, to prevent code being inadvertently added to live systems. Equally, code reviews, including detailed actions such as regression testing, to ensure changes made to the live codebase are correct before deployment, would also likely have mitigated this incident. In line with this, it is recommended that MPS document how code is to be tested, reviewed, and deployed in order to establish best practices that should then be followed going forward. In particular, when this involves software that processes potentially sensitive data.