DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Police Service of Northern Ireland (PSNI)

OF: PSNI Headquarters
65 Knock Road
Belfast
BT5 6LE

1.1 The Information Commissioner (the Commissioner) issues a reprimand to PSNI in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain infringements of the DPA 2018.

The reprimand

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

- Section 34 (3) which states that "the controller in relation to personal data is responsible for and must be able to demonstrate compliance."

- Section 35 (1) which states that "the processing of personal data for any of the law enforcement purposes must be lawful and fair."

- Section 40 which states that "personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures. (And, in this principle, ، 'appropriate security" includes protection against unauthorised or unlawful processing and accidental loss, destruction or damage)."

- Section 42 (1) which states "a controller requires to have an appropriate policy document in place when carrying our sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in Schedule 8."

- Section 73 (1) which states "a controller may not transfer personal data to a third country or to an international organisation unless –

(a) The three conditions set out in subsection (2) and (4) are met, and

(b) in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in the member State, which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State."

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

1.4. It is considered that PSNI failed to have appropriate measures in place to prevent the Extradition Unit (EU) unlawfully sharing personal data, including criminal offence data, with the United States Department of Homeland Security (DHS). This had an impact on 174 data subjects. This unlawful sharing of personal data including basic personal identifiers (such as name and contact details), information recorded within an Electronic System for Travel Authorisation (ESTA) or VISA applications, information relevant to locating missing persons, criminal conviction data, and biometric data, had been taking place since 2016 and continued following the introduction of DPA 2018 until 15 October 2020. Members of staff within the EU had legitimate but insufficiently regulated access to various PSNI systems and were able to extract personal data which was then unlawfully shared with DHS.

Section 34 (3)

1.5. To enable EU staff to perform their duties, access was allowed to multiple systems and policies and procedures were in place to regulate this. However, a culture evolved where sharing was done outside of those processes and it is uncertain whether staff knew their practices were outside policy. The investigation found there was a lack of effective managerial oversight, had this been in place further unlawful sharing of personal data could have been prevented. Therefore, PSNI could not evidence there was adequate oversight or governance in place to demonstrate its accountability with the legislation.

Section 35(1)

1.6. PSNI's fundamental purpose is law enforcement and it is accepted that sharing of data is necessary to facilitate this purpose. Whilst PSNI had a process in place to share information with foreign law enforcement, such as DHS, under its data protection framework, the investigation found that an informal practice had evolved over a number of years where proactive sharing of personal data, including criminal conviction data, was taking place outside of that arrangement. The sharing was intended to alert DHS of individual's intended travel to the US and no

formal process was being followed. PSNI were unable to demonstrate it had a documented reason for proactive sharing, for example following the receipt of a formal request which identified a specified reason, in line with the data protection legislation, for sharing the personal data with the DHS. Data subjects would not reasonably expect their personal data to be used in this way which resulted in data subjects and their family members being refused entry to the US.

Section 40

1.7. Due to the nature of the personal data that was being processed, PSNI should have ensured a higher level of protection and safeguards were in place. The investigation found despite PSNI having polices and guidance in place on how personal data of this type should be handled to ensure the appropriate security of that personal data was applied, EU staff failed to follow the correct process. Personal data was routinely sent to the US via email, without encryption or password protection. Whist there is no evidence to suggest the personal data was inappropriately accessed, the investigation found that personal data was processed without the appropriate security being applied.

Section 42 (1)

1.8. Some of the personal data that was shared with DHS was biometric data and would be considered to be sensitive processing as per section 35 (8) DPA 2018. To ensure sensitive processing is compliant with data protection legislation, PSNI must demonstrate that this processing is strictly necessary, and either have the consent of the data subject or satisfy one of the conditions in schedule 8 of the DPA 2018. An appropriate policy document must also be in place as per schedule 1 part 4 of DPA 2018. The investigation found that data subjects were unaware their data was being processed in this way. Therefore, consent had not been obtained. Sensitive processing was taking place for the purpose of disrupting travel arrangements which resulted in data subjects being refused entry to the US. Processing would not prevent or detect a crime and therefore does not meet the definition of law enforcement purposes. PSNI were unable to satisfy one of the conditions in schedule 8 or provide a copy of an appropriate policy document. Therefore, processing was not lawful or fair.

Section 73 (1)

1.9. EU staff were proactively sharing personal data with DHS to disrupt travel arrangements and that sharing was not necessary for law enforcement purposes. The sharing of personal data in this way would not have prevented a data subject committing an offence but would merely alert the authorities to the possibility that one may take place. PSNI did not have any appropriate safeguards in place. The transfer of personal data was also not for any specified special circumstances.

Therefore, the investigation found the transfer of personal data to be unlawful.

Remedial steps taken by PSNI.

1.10. The Commissioner has also considered and welcomes the remedial steps taken by PSNI in the light of this incident. In particular, in the course of our investigation we have noted that the Professional Standards of the EU and the Police Ombudsman of Northern Ireland (PONI) have conducted a review of the incident and recommendations have been made. PSNI has since introduced stricter controls to improve its compliance. These include ensuring any future data sharing is conducted within a formal arrangement, reviewing existing guidance and polices, and creating a standard operating procedure which includes data transfer. The Commissioner considers these steps to be appropriate and that they should prevent an incident of this nature happening again.

Decision to issue a reprimand

1.11. Taking into account all the circumstances of this case, the Commissioner has decided to issue a reprimand to PSNI in relation to the infringements of sections of the DPA 2018 set out above.

Further Action Recommended

1.12. Due to the length of time since the incident took place the following steps may have already been addressed.

1.13. The Commissioner recommends that PSNI should take certain steps to ensure its compliance with DPA 2018

1. In order to ensure compliance with section 35(1) of DPA 2018, appropriate steps should be taken to ensure a clear lawful basis is identified and documented prior to the sharing of information. Any sharing should take place only through a formal arrangement. Staff should be made aware of the revised guidance to enable them to understand what data can be shared prior to sharing with third parties. PSNI should consider increasing staff knowledge and awareness about data protection through training and refresher training which should take place on a regular basis.

2. In order to ensure compliance with section 34(3) of DPA 2018, access to personal data should be reviewed, and access granted as appropriate and only for as long as is necessary. PSNI should ensure staff understand processes and increase managerial oversight by way of regular audits to improve governance.

3. In order to ensure compliance with section 40 of DPA 2018, when processing personal data for law enforcement purposes, PSNI must

ensure that the appropriate level of security is applied. PSNI should consider reviewing existing internal security procedures to identify if any additional preventative measures can be implemented. PSNI should consider introducing regular management checks to ensure the revised guidance is being adhered to.

4. In order to ensure compliance with section 42 of DPA 2018, when processing sensitive personal data, PSNI must ensure it either has consent for processing or be able to satisfy one of the conditions in Schedule 8. An appropriate policy document must be in place which must explain your procedures for ensuring compliance with the law enforcement data protection principles; and you monitor the retention and erasure of this data. part-3-appropriate-policy-document.docx (live.com)

5. In order to ensure compliance with section 73 of DPA 2018, 73 of DPA 2018, PSNI must identify a lawful bases prior to sharing with third countries ensuring that an appropriate data protection framework is in place. https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/

1.14. The ICO would typically expect PSNI to provide a progress update on the above recommendations within three months of the date of this reprimand. However, PSNI has informed the ICO that it has already taken steps to address each of the recommendations and to improve its compliance with DPA 2018.