DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to the Chief Constable of Sussex Police 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

The Commissioner has decided to issue a reprimand to the Chief Constable of Sussex Police in respect of the following infringements of the DPA 2018:

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

- Section 45(1) which states that "A data subject is entitled to obtain from the controller-
  (a) Confirmation as to whether or not personal data concerning him or her is being processed, and
  (b) Where that is the case, access to the personal data and the information set out in subsection (2)."

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

It is considered that the Chief Constable of Sussex Police failed to give adequate or appropriate consideration to compliance with data protection legislation, either that in place at the time the App was initially introduced or subsequently upon the introduction of the DPA 2018 in respect of the processing of personal information and special category data via use of the App, and specifically:

Section 35(1)

It is acknowledged that the App had initially been requested by a specific cadre of officers. However, whilst it was technically possible for the App to have been assigned to a limited number of officers, which would have limited the scope of the processing of personal information and special category data, Sussex Police chose not to do so, instead making the App available to all staff members. It was stated that a total of 1,015 staff members had downloaded the App and as at 27 April 2021, in excess of 202,000 recordings of telephone conversations had been automatically saved onto their mobile devices. It is considered highly likely that the App captured a variety of data, including sensitive personal data, across a

broad range of topics. It is not known how many of the call recordings relate solely to law enforcement matters. The collection of the data is considered to be unfair and unlawful; and not in all cases strictly necessary for the purposes of law enforcement.

No adequate risk assessment has been undertaken in respect of intended processing of personal information at the time the App was initially made available. From the evidence provided, it was unclear how the App had been approved for release as there was no documentation available for this. Devices onto which the App was downloaded and activated captured calls indiscriminately and without the knowledge of affected data subjects. The processing is considered to have been unnecessary and could have been avoided if Sussex Police had taken steps to limit use of the App and, where it was considered necessary and proportionate for deployment, to have ensured that the personal data and sensitive personal data captured was achieved in a compliant and lawful way.

The list of available Apps was not routinely reviewed and no specific review took place in preparation for a Forces-wide platform change in November 2017. Following the platform change, Apps were not automatically populated onto refreshed mobile devices and required manual addition by individual officers. This is considered to represent a missed opportunity to have reviewed how personal information was being processed and retained as a result of use of the App.

Additionally, no review of the App's availability or the resultant processing of personal information took place when the DPA 2018 was introduced. This is considered to be a further missed opportunity to have ensured that processing being undertaken was in compliance with the newly implemented legislation. This is of particular concern given the enhanced rights afforded to data subjects under the new legislation.

No adequate instruction or guidance was provided by Sussex Police to inform staff how the App functioned or to ensure processing was compliant with its responsibilities as a data controller; or that officers were aware that use of the App constituted processing of personal information under data protection legislation.

The use of the App breached the Forces-issued Electronic Devices policy by using an App to "record notes or other investigative details". However it is noted that no policy of this type was in place when the App was first made available in late 2016. The lack of adequate oversight of the processing of personal information by officers using an approved App is considered to be a failure by Sussex Police, as a responsible data controller, to ensure that processing was compliant with the DPA 2018.

Evidence provided during the ICO's investigation indicated that many of the officers who had downloaded and activated the App were unaware that all calls would be recorded. Recordings were saved locally on devices and were therefore not automatically backed-up, nor was information retained if devices were lost or damaged which would result in the devices being remotely wiped. This calls into question whether all personal information processed during the period the App was in use has been appropriately disclosed as evidential material. This is considered to represent the potential for impact to prosecutions and/or criminal proceedings which would result in potential detriment to affected data subjects. However no evidence was presented to indicate that information contained within the calls would have altered criminal case conclusions.

Section 45(1)

Due to the length of time the App was in use the exact amount of personal information and special category data processed is unknown. It is therefore impossible to accurately assess the number of data subjects affected by the App usage. On the balance of probabilities it is considered likely to be a significant number across a broad range of categories, including victims, witnesses, and perpetrators of suspected crimes.

Data subjects were not informed that their telephone calls were being recorded resulting in them being denied the opportunity to exercise their rights of access under the DPA 2018. These include the right to object to the recording; to otherwise complain; to ensure accuracy of retained information; to request rectification and/or erasure; or to exercise their right of access to personal information in order to obtain transcripts or copies of recordings. On the balance of probabilities it is considered likely that some affected data subjects would have chosen to exercise such rights, had they been aware that processing was taking place. The lack of transparency and fair processing by Sussex Police denied data subjects the right to do so. This is considered to be evidence of a lack of appropriate consideration by Sussex Police to the rights afforded to data subjects under the DPA 2018.

Other compliance concerns

The ICO's investigation identified other compliance concerns that are not subject to the corrective measure being imposed:

Every call made from or received by devices onto which the App had been downloaded and activated was recorded. As stated above, it is considered highly likely that the App captured a variety of data, including sensitive personal data, across a broad range of topics. This is considered to be evidence of an infringement of section 35(4) of the DPA 2018 which states that "Personal data collected for any of the law enforcement

purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law."

The retention of call recordings on officers' mobile devices was not subject to any review or oversight by Sussex Police prior to the matter being identified as a compliance failure. This is considered to be evidence of an infringement of section 37 of the DPA 2018 which states that "personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."

Furthermore, prior to the matter being identified as a compliance failure, the recordings were retained until such time as the individual device was remotely wiped, either as a result of device refresh/upgrade or following the device being reported as lost or stolen. This is considered to be evidence of an infringement of section 39(1) of the DPA 2018 which states that "personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed." This is also considered to be evidence of an infringement of section 39(2) which states that "Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes."

Risk assessments undertaken on other previously approved Apps as part of remedial action following the ICO's investigation of this matter identified an additional App which processed personal information. A subsequently undertaken Data Protection Impact Assessment (DPIA) identified elements of risk and compliance failure. This is considered to be evidence of an infringement of section 40 of the DPA 2018 which states that "personal data processed for any of the law enforcement purposes must be so 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 against accidental loss, destruction or damage)."

While it is acknowledged that the App was downloaded onto officially provided encrypted mobile devices, evidence was provided during the investigation to indicate that copies of call recordings had been manually transferred onto removable media. This raises concerns regarding the ongoing security of the personal information and special category data contained within the recordings, once transferred from the encrypted device. This is considered to be evidence of a further infringement of section 40 of the DPA 2018.

Mitigating factors

In the course of our investigation we have noted that the original rationale for making the App available was that some form of recording software was required to support critical operational policing and it is acknowledged that the App was likely to be beneficial under certain circumstances. However no adequate consideration of compliance with data protection legislation had been undertaken prior to making the App available to officers. If this consideration had been given, it is likely that risks could have been mitigated.

Remedial steps taken by Sussex Police

The Commissioner has also considered and welcomes the remedial steps taken by Sussex Police in the light of this incident. In particular that a Gold Group, chaired by an Assistant Chief Constable, was promptly formed upon identification of the matter. In addition, the App has been withdrawn from use and recordings, other than those submitted to the Crown Prosecution Service or otherwise considered to be evidential material, were promptly destroyed.

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 the Chief Constable of Sussex Police in relation to the alleged infringements of sections 35(1) and 45(1) of the DPA 2018 set out above.

The ICO considered notifying the Chief Constable of Sussex Police of its intention to impose an administrative penalty in the amount of £1.0 million. However, since June 2022 the ICO has adopted a revised approach to public sector enforcement and, on this occasion, we have decided not to impose an administrative penalty.[1]

Further Action Recommended

The Commissioner recommends that the Chief Constable of Sussex Police should take certain steps to ensure its compliance with the DPA 2018. With particular reference to sections 35(1) and 45(1) of the DPA 2018, the following steps are recommended:

1. The consideration and deployment of any new Apps should be assessed by a specific team with adequate and appropriate consideration given to the method and means of processing, and any affects this will have on data subject rights.

[1] ICO sets out revised approach to public sector enforcement | ICO.

2. The above process should be documented and authorised at appropriate level, with remedial action taken to ensure the processing is compliant with current legislation prior to the App being deployed.

3. Adequate instruction and guidance should be issued to staff in respect of the use of any App, with officers required to confirm that issued instruction and guidance has been read and understood in order for Sussex Police to be satisfied that officers are aware of their compliance responsibilities during App usage.

4. In light of this incident, review existing policies and procedures to ensure that adequate consideration has been given to data subject rights during the processing of personal information and special category data. Policies and procedures that are applicable across multiple Forces should be clearly marked as such, and responsibilities defined for the routine review and uplift, if required, of content.

5. In light of this incident, conduct a review of the content of data protection training, particularly that in respect of law enforcement processing, to ensure sufficient prominence is given to the requirement for consideration of data subject rights.

The Commissioner requires the Chief Constable of Sussex Police to provide details of the actions taken to address the above recommendations within three months of receipt of this reprimand, and by no later than **4 July 2023**.