**DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION**

**REPRIMAND**

## TO: Chief Constable of Kent Police

**OF:** Kent Police Headquarters, Thames Way, Northfleet, Gravesend, Kent, DA11 8BD

1.1 The Information Commissioner (the Commissioner) issues a reprimand to the Chief Constable of Kent Police in accordance with Article 58(2)(b) of the UK General Data Protection Regulation (UK GDPR)/ Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain alleged infringements of the DPA 2018.

## The reprimand

1.2 The Commissioner has decided to issue a reprimand to the Chief Constable of Kent Police (Kent Police) in respect of the following infringement of the DPA 2018:

- Section 40 which states that "The sixth data protection principle is 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)".

## Background

A reprimand is being issued to Kent Police in respect of an incident in February 2021 when a Kent Police officer took a photograph of an individual's identity document using her personal mobile phone and uploaded the image onto Telegram, a social media application (the App). From the evidence provided to the ICO, the Telegram distribution group onto which the image was uploaded was being used by multiple UK police forces and international law enforcement agencies for the purpose of combatting vehicle crime. The Kent Police officer did not inform the individual that further processing of his personal data would take place; how it would be processed; or the purpose for doing so.

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

1.4 Whilst acknowledging Kent Police's statement that the use of the App was not officially sanctioned, it is noted that at the time of the incident 25

officers were known to have downloaded the App onto their personal devices and were members of the distribution Group. The Commissioner understands from the evidence provided by Kent Police that 25 of its officers were members of the group at the time of its discovery, however it is maintained by Kent Police in representations that only five of these officers had previously used the Telegram app to share personal data. At the time of the ICO's investigation it was stated that there were a total of 241 Group members, with Kent Police making up almost 10% of the membership. It is further noted that two Kent Police officers had administration rights for the Group for moderation purposes. Given the length of time that the Group had been in use, it has not been possible to ascertain if any other Kent Police officers had, prior to the investigation commencing, previously used the Group but, from the evidence provided, it is considered likely that officers had been members of the Group for a significant period of time.

1.5 It is of concern that the sustained use of such a tool could have gone unnoticed by supervisors, which is considered to be indicative of a lack of awareness of data protection responsibilities, both at operational and supervisory level. This represents a failure on the part of the Chief Constable of Kent Police, as the data controller, to have adequately informed all staff of their responsibilities under data protection legislation in order that such inappropriate use could have been identified more promptly.

1.6 Data controllers are responsible for ensuring that their employees are adequately informed of their personal responsibilities in complying with data protection legislation when performing their official duties. It was Kent Police's responsibility to ensure that officers were adequately informed that the use of personal devices to process data obtained as part of their official duties was not acceptable and that personal devices should not have been used to process personal data for law enforcement purposes. The ICO considers that the number of Kent Police officers who were members of the Group and the sustained length of time over which the Group had been active, to be evidence that this was not an isolated incident as a result of individual human error on the part of one officer. Instead, the ICO investigation found that Kent Police failed to ensure relevant information had been adequately and appropriately communicated in order that officers acted in compliance with published policy, thereby processing personal data in compliance with current data protection legislation.

1.7 In response to enquiries it was stated that there was not a policy in place to advise officers on the procedure for ascertaining the veracity of ID documents. It is noted that this was despite Kent Police's acknowledgement that seeking advice from European counterparts "can be slow". However it is also acknowledged that such advice was only

normally sought when documents were seized, which was not the case in the incident under investigation and that in this case the Kent Police officer had "considered that all possible official avenues of verification had been exhausted". This is considered to be a failure by Kent Police, as a responsible data controller, to ensure that adequate guidance was available to staff members with respect to the processing of personal data in compliance with data protection legislation. The lack of a written policy or other procedural documentation is considered to represent a missed opportunity to have prevented the incident from occurring.

1.8 It is noted that while the ICT Acceptable Use Policy (the Policy) focuses primarily on officially provided equipment, there is only brief reference to personal devices and indicates that there are exceptions whereby the use of personal devices would be permitted to afford flexibility for officers in front-line situations. However it is also noted that in response to enquiries regarding the Policy, Kent Police stated usually officers needed to make operational decisions based on circumstances; that it was not always necessary to request permission but that officers would be required to justify their use when questioned. Kent Police stated that an example would be a situation where an officer did not have their officially provided device with them but needed to record an incident in progress, or take a photograph, or make an operationally sensitive call. It is noted that the use of the Telegram Group does not fall within these parameters. In further response, Kent Police stated it was not aware of any such requests for exceptional use, noting that if such requests had been received a "suitable approved device" would have been provided rather than agreement to the use of a personal device being given.

1.9 Whilst it is acknowledged that the use of the Group via personal devices was not envisaged by Kent Police to be an example of an exception that permitted such use, the ICO considers that the length of time during which the Group had been in use, in combination with the number of Kent Police officers who were members of the Group, to indicate that officers had proceeded to use their personal devices without seeking relevant authorisation to do so. Whilst this could be considered to be multiple instances of officers failing to comply with published policies, the ICO considers this to be evidence of an organisational failure to adequately inform officers that such use was not acceptable.

1.10 Additionally, the use of personal devices is considered to represent a potential security weakness. In this instance, the use of the Group also resulted in data potentially being uploaded to Telegram as a result of messages being stored as "cloud chats" on Telegram's servers, which are hosted internationally. Therefore access to the personal data shared via Telegram cannot be considered to be securely held or access adequately restricted.

1.11 Furthermore, due to the lower level of security afforded to the majority of personal devices compared to those officially provided, the personal data processed could be at risk of hacking or access by individuals who are not police or law enforcement officers. In the absence of a detailed policy to explain how such personal device usage should be managed this is considered to be an area of potential weakness in respect of the security of any personal data processed on an officer's personal device.

1.12 It was stated that all officers and staff were required to confirm their understanding of published policies and procedures before being granted access to official system and that documentation would be recirculated when updated or amended. However it was not stated if officers were required to re-confirm their understanding following each update and no evidence as to how this was centrally recorded has been provided. This is considered to be a missed opportunity by Kent Police to have ensured that officers were adequately aware that the use of personal devices for official business was not sanctioned.

1.13 While acknowledging that the Kent Police officer uploaded personal data to the Group for the purpose of verifying an individual's identity, and that policies, procedures and data protection training were in place, it is noted that the Group had originally been set up for the purpose of combatting vehicle crime and the period of time during which the Group was in use by employees, without challenge, is considered to be indicative of a lack of organisational awareness among staff of their responsibilities under data protection legislation.

Mitigating factors

1.14 In the course of our investigation we have noted the Chief Constable of Kent Police's statement that Telegram was not an officially provided or approved App; that it was blocked on officially provided mobile devices; and that Kent Police was unaware of the use of the App by officers prior to the incident being reported.

Other compliance concerns

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

1.16 It is noted that affected data subjects were not informed of the unauthorised processing or that their personal data may be shared with overseas law enforcement agencies via officers' use of the Telegram distribution Group. This lack of transparency will impact on data subject rights under the DPA 2018: the right to be informed, the right of access, the right to rectification, the right to erasure, and to restrict processing. It

is considered likely, on the balance of probabilities, that the personal data of a significant number of data subjects will have been processed since the Group's introduction in 2016.

1.17 While acknowledging that the personal data was being processed for law enforcement purposes, there was still the potential for distress to be caused had data subjects been aware that their data was being processed via social media. However Kent Police could be considered fortunate that no evidence has been provided of actual detriment as a result of its officers' use of the Group.

Remedial steps taken by Kent Police

1.18 The Commissioner has also considered and welcomes the remedial steps taken by Kent Police in the light of this incident. In particular that the incident was promptly brought to the attention of the organisation who had initially created the Group and the ICO; that officers were instructed to stop using the Group; and that disciplinary action had been taken in respect of those officers who were identified as having used the Group.

Decision to issue a reprimand

1.19 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 Kent Police in relation to the infringement of section 40 of the DPA 2018 set out above.

## Further Action Recommended

1.20 The Commissioner has set out below certain recommendations which may assist the Chief Constable of Kent Police in rectifying the infringements outlined in this reprimand and ensuring Kent Police's future compliance with the DPA 2018. Please note that these recommendations do not form part of the reprimand and are not legally binding directions. As such, any decision by Kent Police to follow these recommendations is voluntary and a commercial decision for Kent Police. For the avoidance of doubt, Kent Police is of course required to comply with its obligations under the law.

1.21 If in the future the ICO has grounds to suspect that Kent Police is not complying with data protection law, any failure by Kent Police to rectify the infringements set out in this reprimand (which could be done by following the Commissioner's recommendations or taking alternative appropriate steps) may be taken into account as an aggravating factor in deciding whether to take enforcement action - see page 11 of the

Regulatory Action Policy Regulatory Action Policy (ico.org.uk) and article 83(2)(i) of the UK GDPR/section 155(3)(e) of the DPA 2018.

1.22 The Commissioner recommends that Kent Police should consider taking certain steps to improve its compliance with the DPA 2018. With particular reference to section 40 of the DPA 2018, the following steps are recommended:

1. Regularly review the ICT Acceptable Use Policy to ensure that sufficient prominence is given to approved circumstances of use of personal devices, with clear guidance for staff on appropriate measures to be taken to ensure processing is in compliance with data protection legislation.

2. Regularly review the procedure for issuing updated guidance, policies and procedures to ensure that such updates are read and understood by all staff, with compliance adequately monitored and recorded.

3. Regularly review the content of data protection training to ensure it is adequate for the purpose of informing all staff of their responsibilities in respect of compliance with data protection legislation. Consider including guidance on what Kent Police considers to be acceptable use of personal devices and generic details of this incident as an example of how breaches can, and do, occur.

4. Provide guidance and training around the force-wide use of social media Apps to ensure compliance on force devices with data protection legislation, and to ensure awareness of prohibited actions on personal devices, taking appropriate action to restrict or prevent future use if compliance failures, are identified.

The ICO invites Kent Police to update the ICO on the progress of implementing the recommendations made.

Date: 5 March 2024