DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Dover Harbour Board

OF: Harbour House, Waterloo Crescent, Dover, Kent, CT17 9BU

1.1 The Information Commissioner (the Commissioner) issues a reprimand to Dover Harbour Board 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 infringements of the DPA 2018.

The reprimand

1.2 The Commissioner has decided to issue a reprimand to Dover Harbour Board 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 40 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)";

Background

A reprimand is being issued to Dover Harbour Board in respect of the creation and use of a social media distribution group, initially created in WhatsApp but later migrated to Telegram. From the evidence provided to the ICO, the distribution groups were used by multiple UK police forces and international law enforcement agencies for the purpose of combatting vehicle crime.

The distribution groups were created by an officer from the Port of Dover Police. The Port of Dover Police is a non-Home Office Constabulary that is funded entirely by the Port Authority, Dover Harbour Board, to provide a general policing service at the Port of Dover. Dover Harbour Board advised the ICO the constables of the Port of Dover Police are its employees. Therefore it is considered that Dover Harbour Board is the relevant data controller in respect of this matter.

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

1.4 This reprimand concerns the processing of personal data and special category data via the creation and use of a social media distribution group (the Group) initially created on WhatsApp and subsequently transferred to Telegram in 2020. Dover Harbour Board is of the opinion that no personal data has been processed during members' use of the Group. However from the evidence provided, the ICO does not share this view. It is considered that Dover Harbour Board failed to give adequate or appropriate consideration to compliance with data protection legislation, either that in place at the time the Group was created on WhatsApp or subsequently upon the introduction of the DPA 2018. The use of the Group began prior to the implementation of the DPA 2018 however for the purpose of this reprimand, the period of contravention is considered to be May 2018 until February 2021, and specifically:

1.5 The Group was initially created by an officer from the Port of Dover Police (Officer A) using his personal mobile phone for the purpose of combatting vehicle crime. Multiple senior officers supervising the officer who set up the distribution Group were aware over the timeframe during which the Group existed of his intention to create, promote and use the Group. However no evidence has been provided to demonstrate that adequate consideration was afforded to compliance with data protection legislation nor were members of the Group informed about data protection requirements. Officer A's supervisor had removed himself from the WhatsApp Group prior to its migration to Telegram due to the volume of messages being processed but was aware of the continuation of the Group on Telegram. Officer A also stated that several of his supervising officers during the lifetime of the use of the Group had been members of it, which is considered to be further evidence of supervisory management awareness of both the existence of, and purpose of, the Group on WhatsApp and Telegram over a sustained period of time. This is considered to be evidence of inadequate awareness of, or compliance with, data protection considerations on a corporate level and represents an infringement of section 40 of the DPA 2018.

1.6 It was stated that the Group was migrated from WhatsApp to Telegram as a result of several members of the Group having suggested that Telegram was a more secure network. However, it is understood that although the App is encrypted the default user settings do not have adequate encryption automatically activated, with users being required to individually implement privacy settings. It was noted that if these are not understood or implemented correctly, the content of chats, files and shares can be placed at risk, with most messages being cloud chats which are stored on Telegram's servers and can be accessed by Telegram. The

servers were noted to be hosted in the Netherlands although the possibility for data to be shared to Dubai or other parent company owned locations was also noted. Therefore access to the personal data shared via Telegram cannot be considered to be securely held or access adequately restricted which is considered to represent an infringement of section 40 of the DPA 2018.

1.7 Access to the Group was via the personal mobile devices of Port of Dover Police officers and no information in respect of privacy settings or data security was provided to Group members. It is therefore likely that personal data relating to individuals about whom intelligence was being sought would be saved on these personal devices in the form of photographs and message content. Officially provided devices routinely have enhanced levels of security and encryption that are not usually present on personal devices, unless specifically implemented by users. While it is acknowledged that Dover Harbour Board had no control over security settings on its officers' personal devices, the lack of enhanced security measures is considered to be weakness in respect of the security of personal data being processed for official purposes and data held on personal devices would potentially be at risk of access by third parties. This is considered to be evidence that Dover Harbour Board has not ensured the appropriate security of personal data being processed for official purposes as required by section 40 of the DPA 2018.

1.8 Dover Harbour Board stated there was no evidence that a risk assessment was undertaken either upon the setting up of the WhatsApp Group or its migration to Telegram and that no Terms of Reference for the Group had been published. Furthermore, that there was no written constitution for the Group and little supervision of it; there was no real oversight of members or individual posts that were made; there was no process in place for removing members from the Group who left law enforcement employment; and those with administration duties for the Group were unclear of their role and no training was provided. The lack of evidence of adequate safeguards being in place with respect to membership and constitution of the Group is considered to be evidence of a lack of appropriate records management in place for a forum designed to share personal data. This demonstrates an overall lack of consideration for, and compliance with, data protection legislation which represents an infringement of section 40 of the DPA 2018.

1.9 A total of 241 officers were members of the Group, which together with the nature of the personal data being shared, is evidence of the potential for wide-ranging impact on affected data subjects. Affected individuals were not informed that their personal data was being processed on a social media App or that copies of their personal data were being uploaded, and would have no reasonable expectation of this occurring. This raises concerns with respect to transparency and a denial

of data subject rights and represents an infringement of section 35(1) of the DPA 2018.

1.10 Dover Harbour Board provided evidence of data protection training undertaken by staff, which was stated to be mandatory and undertaken annually. However the content made no reference to the processing of personal data for law enforcement/policing purposes; and made no specific reference to the processing of personal data by policing organisations. Dover Harbour Board provided no evidence that prior to the incident occurring data protection training in respect of the processing of personal data for law enforcement/policing purposes was made available to staff. While the training evidenced is considered adequate to give a broad overview of the principles of data protection, and the content adequate for a commercial organisation handling minimal amounts of personal data, it is not considered adequate for operational policing purposes. It is considered that additional information specifically in respect of law enforcement/policing purposes as set out in the DPA 2018 would be required in order for an officer to be sufficiently informed of their responsibilities in respect of compliance with current legislation. Furthermore, relevant policies provided by Dover Harbour Board did not provide on review, enough information on the use of social media that could serve to educate officers on the correct handling procedures for official purposes. These issues are indicative of a lack of corporate awareness of the content of training and policies; a failure to ensure staff have received appropriate data protection training; and a lack of adequate awareness of data protection legislation requirements. This is supported by the fact that none of the supervising officers who were stated to be aware of the existence of the Group identified that use of it was likely to contravene data protection legislation and is considered to be evidence of an infringement of section 40 of the DPA 2018.

Remedial steps taken by Dover Harbour Board

1.11 The Commissioner has also considered and welcomes the remedial steps taken by Dover Harbour Board in the light of this incident. In particular.

1.12 All officers from Port of Dover Police were instructed to cease all activity linked to the Group on 17 February 2021.

1.13 All officers would undertake a higher level of training in respect of knowledge of data protection legislation. Additionally, Port of Dover Police officers had been enrolled on the College of Policing's online training regarding the requirements of the DPA 2018 in relation to the processing of personal data for law enforcement purposes.

1.14 The Board would consider whether further guidance should be given to staff on the type of information that might be shared during the use of social media groups.

1.15 Dover Harbour Board's IT department should give instruction to all officers who still had the WhatsApp/Telegram Apps on how to delete associated data.

Decision

1.16 Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to Dover Harbour Board in relation to the infringements of sections of the DPA 2018 set out above.

1.17 The ICO considered notifying Dover Harbour Board of its intention to impose an administrative penalty in the amount of £500,000. 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

1.18 The Commissioner has set out below certain recommendations which may assist Dover Harbour Board in rectifying the infringements outlined in this reprimand and ensuring Dover Harbour Board's future compliance with the UK GDPR and 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 Dover Harbour Board to follow these recommendations is voluntary and a commercial decision for Dover Harbour Board. For the avoidance of doubt, Dover Harbour Board is of course required to comply with its obligations under the law.

1.19 If in the future the ICO has grounds to suspect that Dover Harbour Board is not complying with data protection law, any failure by Dover Harbour Board 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) DPA 2018.

1.20 The Commissioner recommends that Dover Harbour Board should consider taking certain steps to improve its compliance with the DPA

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

2018. With particular reference to sections 35(1) and 40 of the DPA 2018, the following steps are recommended:

1. Review existing policies and procedures to ensure that content is adequate in respect of compliance with data protection legislation. Particular consideration should be given to data subject rights during the processing of personal data and special category data for policing purposes.

2. Conduct a review of the content of data protection training to ensure that training provided is relevant to, and adequate for, the staff members receiving it. Ensure that all Port of Dover Police officers are provided with, and undertake, training that includes adequate information in respect of the processing of personal data for law enforcement purposes, ensuring that sufficient prominence is given to the requirement for consideration of data subject rights.

3. Adequate instruction and guidance should be issued to staff in respect of the use of any officially approved App, particular those with links to social media, with employees and Port of Dover Police officers required to confirm that issued instruction and guidance has been read and understood in order for Dover Harbour Board to be satisfied that all staff are aware of their compliance responsibilities during App usage.

4. Conduct an investigation into the use by staff of other social media groups. If use of any is found, produce clear instructions for staff to follow in respect of the use of personal devices and the processing of personal data gathered as a result of usage in order to ensure future compliance with data protection legislation.

The ICO invites Dover Harbour Board to update the ICO on the progress of implementing the recommendations made.

Date: 5 March 2024