Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

OFFICIAL SENSITIVE

[redacted]
Department of Health and Social Care
[redacted]

By email only to: [redacted]

11 July 2022

Reference: INV/0694/2021

Dear [redacted],

I write further to our meeting of 21 June 2022 and related correspondence.

As explained, the Information Commissioner's Office (ICO) has concluded its investigation into the use of private correspondence channels by the Department of Health and Social Care (DHSC), and we have shared, in confidence, our proposed draft report for Parliament about this matter.

Within that report, it is explained that the ICO has issued the DHSC with a reprimand in relation to data protection compliance matters under the General Data Protection Regulation (GDPR), the UK General Data Protection Regulation (UKGDPR) and the UK Data Protection Act 2018 (DPA). This letter sets out the detail of that reprimand.

Our consideration of this case

Key compliance issues

It is important to stress that the ICO does not take the view that the DHSC, and public bodies in general, should *never* send information containing personal data to private communication channels. However, where such channels are in use and the processing of personal data is taking place, they should be operated in compliance with the requirements of UK data protection law.

As set out in our proposed report to Parliament, our investigation has determined that private communication channels were in regular use by the Department and that the communications exchanged via these channels were not insignificant in number.

Of those communications, most if not all of the messages sent and received contained personal data. Typically, such data consisted of names, contact details, and information related to individuals' work in a professional capacity.

In a very small number of examples, we have identified special category data in such communications. These examples included: a reference to the medical situation of a family member when emailing a Minister; and a reference to an individual's political party membership (this was referenced in an email relating to Government business and was redirected to official systems and reflects that Ministers operate in both official and political capacities). A further example was identified of an email that contained special category data of the identity of the first person in the UK to receive a Covid vaccine, however we note that information was already in the public domain.

As such, we have concluded that special category data was not processed via private communication channels to any significant degree. Whilst this is reassuring, it does not negate the fact that personal data was regularly sent and received via such channels, despite official accounts within the control of the DHSC being available.

We have therefore found that the DHSC did not fully comply with the following requirements of the GDPR, UK GDPR and DPA18:

- **Article 5(1)(e) –** Storage limitation
- **Article 5(1)(f)** – Security
- **Article 25** – Data Protection by Design and Default
- **Article 32 –** Security of processing

This is because the use of private correspondence channels was taking place, without appropriate controls in place to sufficiently manage the risks such processing presented.

Significant contributing factors to the above infringements include:

- Whilst there were local DHSC policies in place, which stated that the use of private communication channels was prohibited (except in exceptional

circumstances) such polices did not apply to Ministers or Non-Executive Directors (NEDs).

- The Cabinet Office guidance on the use of private communication channels guidance did however apply to Ministers and Civil Servants. This created a disconnect between DHSC polices as applied to employees, and those as applied to Ministers and NEDs.

- Within the Cabinet Office guidance applicable at the time, it was explained that Departments' own security policies would apply when generating and communicating information.

- As such, there was a lack of consistency of application of the Departments policies, including the DHSC Information Management and Acceptable Use of ICT Policies, and that of the application of the Cabinet Office's guidance. We consider that achieving consistency is essential if the DHSC's expectations of Ministers and senior staff in relation to private communication channel use is to be clear to all relevant parties.

- The Department did not have appropriate organisational or technical controls in place to ensure effective security and risk management of private communication channels. This is because controls to mitigate the risks of using private correspondence channels, where such use could not be avoided, were absent.

- Our investigation determined that official government material containing personal data was held on platforms not owned or managed by the Department, despite the users of those platforms being provided with official DHSC accounts. This demonstrates an accumulation of information, including personal data, held outside of the DHSC estate and therefore outside of the Department's direct control. The use of private correspondence channels created an unnecessary level of risk which could easily have been negated if the DHSC had relied on @dhsc.gov.uk issued accounts, which had in any event been provided, to communicate with Ministers and NED's. Reliance on official only accounts would have had the effect of reducing the risk of inappropriate access, a potential loss of integrity or confidentiality, or data loss.

- In addition, the ICO found that smaller volumes of information either marked Official Sensitive or containing Official Sensitive material, was also sent to accounts outside of the DHSC estate, despite those account holders being provided with official DHSC email accounts. These emails contained

personal identifiers consisting of names and contact details of the persons with whom the emails were exchanged. This raises wider security concerns about sensitive departmental material being shared outside of the department with no obvious controls in place. The Government Security Group (part of the Cabinet Office) have therefore been informed of this matter.

- In summary, the use of such channels presented unnecessary risks to the confidentiality, integrity and accessibility of the data exchanged.

We except that the use of private correspondence channels may have brought initial operational benefits at a time in which the UK was facing exceptional pressures at the start of the COVID-19 pandemic. However, it is of concern that such practices were undertaken, with little oversight or evidence of consideration of the risks this might present and application of mitigation measures to minimise those risks.

Investigation outcome

After careful consideration and based on the information provided to date, the Commissioner has decided to issue DHSC with a reprimand in accordance with Article 58 of the UKGDPR.

To confirm, this reprimand has been issued in respect of the following processing operations:

- **Article 5(1)(e) Storage Limitation** requires that personal data be *'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'.*

- **Article 5(1)(f) Integrity and Confidentiality** requires that personal data be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.*

- **Article 25** states '*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

  The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

  An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article'.

- **Article 32 – Security of processing**. This states '*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: …(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services'.*

Further action recommended

We note and welcome the DHSC's acknowledgment of the challenges presented by the inconsistency of application in policies and procedures relating to private correspondence use, and the need to align departmental and cross-government guidance to ensure consistency.

Alongside the ICO's decision to issue DHSC with a reprimand in this case, the Commissioner also recommends DHSC takes additional steps to improve its compliance with the (UK) GDPR and to implement sufficient technical and organisational measures to ensure a level of security appropriate to the risk to the security, integrity, availability and resilience presented in relation to its use of private correspondence channels. In particular, we recommend that the DHSC take the following steps:

(1) In order to improve compliance with article 5 (1) (f) and article 32 of the UKGDPR, the DHSC should undertake a review to assess the security and access controls in place in relation to the platforms in regular use (Google Mail, Hotmail, Whatsapp) when exchanging communications that contain personal data, and to confirm their appropriateness and suitability to support DHSC's compliance with the UKGDPR and DPA18.

(2) As part of that review process, to assess the aforementioned platforms terms and conditions and privacy notices to understand how information would be processed, where it would be stored, and to consider any implications for (a) the security of those platforms in relation to the potential for third party access, (b) the extent to which storage limitation is place, (c) the extent to which the data protection by design and default requirements can be met if use of the platforms is to continue.

(3) The DHSC should also require users of the platforms to adhere to appropriate security guidance, such as that issued by the National Cyber Security Centre (NCSC) with regard to:

- Minimum authentication requirements, for example, two factor authentication controls; and
- Remote access controls (taking into account the ability to access from multiple devices; and to remain logged into accounts)

(4) The Department should also review secure 'bring your own device' options for controlled access to official DHSC accounts via personal devices, in line with NCSC Guidance.

(5) In order to improve compliance with article 5 (1) (e) of the UKGDPR, the DHSC should limit the situations under which such accounts

(Google Mail, Hotmail, Whatsapp) can be used to prevent routine processing on such platforms.

(6) In addition, the DHSC should set clear requirements for the deletion of information from personal accounts once added to the official record.

(7) Further, the DHSC should ensure that the use of personal devices when exchanging personal data adheres to data minimisation principles.

(8) In order to improve compliance with Article 25 of the UKGDPR, the DHSC should extend the application of DHSC specific policies and procedures relating to email use to all holders of @dhsc.gov.uk accounts as standard (including to Non-Executive Directors and Ministers). If this is not possible, tailored information to official account holders exempted from the policies, should be provided as part of their induction processes.

For completeness, we ask that DHSC provides a progress update on the extent to which it has implemented any of the above recommendations to the ICO by no later than 14 October 2022. A further update on progress is requested by no later than 06 January 2023.

We should be grateful if the DHSC could copy their response to the ICO in relation to the above recommendations to the DHSC Select Committee. This will have the effect of placing the response in the public domain, which we hope will bring an additional layer of public confidence in the steps taken.

Unless otherwise instructed, please provide these updates to [redacted]

It must be emphasised that the ICO's decision to issue a reprimand in this case does not detract from the seriousness of this matter and has been reached on the balance of all information available to our office prior to and following the DHSC's and other relevant parities' responses to the Information Notices, our consideration of the correspondence we have exchanged, and the details discussed in the meetings held in support of this investigation.

Therefore, whilst the above measures are our recommendations, if further information relating to the compliance concerns highlighted in this latter comes to light, or if any further incidents or complaints of a similar nature are reported

to us, we will revisit this matter and formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

As you know, there is an intention to publish the outcome of this investigation by way of a report to Parliament. We may also make details of the reprimand itself public.

More generally, we will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/aboutthe%20ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Finally, on behalf of the investigation team I would like to thank you and your colleagues for your assistance during the course of our investigation. We now consider the investigation to be closed.

Yours sincerely,

Steve Eckersley

Director, Investigations

Information Commissioner's Office