

INFORMATION NOTICE

INV/0694/2021

**THE DATA PROTECTION ACT 2018
PART 6, SECTION 142**

Dated 05 July 2021

**To: Department of Health and Social Care
39 Victoria Street
London
SW1H 0EU**

-
1. In exercise of her powers under section 142(1) of the Data Protection Act 2018 ("DPA"), the Information Commissioner ("the Commissioner") requires the Department of Health and Social Care (DHSC) to provide her with the information set out in Annex 1 within 30 days of the date of this Notice.
 2. This Notice is issued under section 142(1) (a) of the DPA.
 3. The information is required for the purposes of carrying out the Commissioner's functions under the data protection legislation to monitor and enforce the application of the UK General Data Protection Regulations ('UK GDPR'). In particular, the Commissioner requires the information set out in Annex 1 for the following reasons:
 - To determine the Department's compliance with the requirements of the UK GDPR in relation to the use of the private email accounts or other electronic private channels of communication (such as Google Mail, Hotmail, Yahoo Mail, WhatsApp or similar) for Departmental business.
 - To examine the Department's compliance with Articles 5 (1) (a), (b), (c), (d); Articles 12-22; Article 24; Article 25; Article 30; Article 32; and Article 35 of the UK GDPR.

4. Following a number of media reports, and complaints received by her office, the Commissioner has concerns that government officials, Ministers, the former Secretary of State, special advisors or any other relevant parties at DHSC have been using private email accounts (or other private channels of communication such as WhatsApp) to conduct Departmental business.
5. The Commissioner's suspicions are based predominately on a series of consistent reports in the media that during at least the time of the COVID-19 pandemic, senior individuals at the DHSC, have conducted official Departmental affairs from private, non-departmental email accounts, or other private channels of communication. Most recently, for example, the considerations of government contracts¹ and the routine use of email² for official business³.
6. The Commissioner wishes to determine that when processing any personal data held in such accounts, the appropriate controls and safeguards are in place to achieve the necessary compliance with the UK GDPR.

Consequences of failing to comply with this Information Notice

7. If a person fails to comply with an Information Notice the Commissioner may serve a Penalty Notice to that person under section 155(1)(b) of the DPA requiring payment of an amount up to £17,500,000, or 4% of an undertaking's total annual worldwide turnover, whichever is higher.
8. Where a person fails to comply with an Information Notice the Commissioner may also apply to the court under section 145(1) of the DPA for an order requiring the person to provide the information referred to in the notice, or other relevant information the Commissioner requires. A failure to comply with an order made under section 145(2) of the DPA will constitute a contempt of court.
9. It is a criminal offence under section 144 of the DPA for a person, in response to an Information Notice, to knowingly or recklessly make a statement which is false in a material respect.
10. It is a criminal offence under section 148(2) of the DPA for a person in receipt of an Information Notice to cause or to permit or to destroy,

¹ <https://www.theguardian.com/politics/2021/jun/29/uk-health-minister-used-private-emails-for-government-business-no-10-admits>

² <https://www.independent.co.uk/news/uk/politics/matt-hancock-email-james-bethell-b1874711.html>

³ <https://www.theguardian.com/politics/2021/jun/28/health-minister-helen-whately-used-private-email-for-government-work-matt-hancock>

dispose of, conceal, block or falsify information with the aim of preventing the Commissioner accessing the requested information.

Right of Appeal

11. By virtue of section 162(1)(a) of the DPA, there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights). If an appeal is brought the information requested in Annex 1 need not be provided pending determination or withdrawal of that appeal. Information on the appeals process is set out in Annex 2.
12. Any Notice of Appeal should be served on the Tribunal within 28 days of the date of this Notice.
13. Information concerning further statutory provisions relating to this Notice is set out in Annex 3.

Signed ..  ...

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Annex 1

INFORMATION REQUIRED TO BE PROVIDED TO THE COMMISSIONER

This Notice requires that the Commissioner be provided with the information described below:

Principles relating to the processing of personal data (Article 5) and the Responsibility of the Controller and Data Protection by Design and Default (Articles 24 and 25).

1. Please provide a copy of the Department's present policy on the use of non-departmental email (or other electronic private channels of communication such as WhatsApp) for official business, and any previous policies held from 01 March 2020. In the event that a policy is not held, please explain the Department's expectations in this regard.
2. Please explain how the above policy/expectations are communicated to staff [and provide copies of all such communications in the last two years preceding the Notice (i.e. from 05 July 2019 to 05 July 2021)], including recordings of oral communication (eg such as Teams or Zoom presentations or similar).
3. Please provide copies of any decision making documents discussing the use of private email (or other private channels of electronic communication such as WhatsApp) accounts for senior staff, government officials, Ministers, the former Secretary of State, special advisors or any other relevant parties at DHSC.
4. Please provide details of the Department; to include the Departmental Private office, and including names & roles of senior staff; reporting lines; and identifying any specific responsibilities for the award of NHS contracts associated with the COVID-19 pandemic.
5. Please provide copies of any internal correspondence related to the use of non-departmental private accounts (or other private channels of communication such as WhatsApp). This should include any summaries made by private office staff or other officials to reflect exchanges they have had with senior staff, government officials, Ministers, the former Secretary of State, special advisors or any other relevant parties at DHSCs.

6. Please confirm whether the Department is (a) aware of, or (b) sanctioned the use of any non-departmental personal email accounts, or other electronic messaging platforms (such as WhatsApp) for the exchange of personal data relating to the work of the Department, for the period 01 March 2020 to 05 July 2021, including but not limited to:

- i. The proposal, discussion, or approval of decisions that require input from senior staff, government officials, Ministers, the former Secretary of State, special advisors or any other relevant parties in relation to Departmental or government contracting, procurement or tenders. This should include any such documents (where they contain personal data) that pertain to COVID-19 matters;
- ii. The arranging of meetings;
- iii. The recording or exchange of minutes of meetings or calls;
- iv. Any other official business conducted by the Department;

7. In the event of the existence of such accounts containing personal data please confirm:

- i. The lawful basis for the processing of personal data on which the Department is seeking to rely. Where special category data is included, please additionally explain the lawful basis for such processing;
- ii. How many accounts are in use and which platforms they concern (for example Google Mail, Hotmail, Yahoo Mail, WhatsApp or similar);
- iii. Of those, how many belong to Departmental staff;
- iv. Where not related to Departmental staff, a description of the relationship between the Department and the account holder;
- v. Confirmation of any private email addresses used to contact senior staff, government officials, Ministers, special advisors or any other relevant parties at DHSC;
- vi. A list of relevant staff and roles in relation to any such accounts;
- vii. The categories of personal data included in the data held and where possible, an approximate number of data subjects to whom the data relates;

- viii. Whether the use of such accounts was officially sanctioned within the Department and if so by whom and when;
- ix. Whether any contracts of use between the platform providers, the account users, or the Department are in place. If so, please provide copies;
- x. Whether terms and conditions of use are in place in relation to the accounts. If so, please provide copies;
- xi. The Department's understanding of where data held in the accounts is hosted, and specifically whether any data is held outside of the UK;
- xii. Whether the Department's Data Protection Officer ('DPO') was aware of the use of such accounts.

Security of processing (Article 32)

- 8. In the event that such accounts are held, please provide details of any (a) technical and (b) organisational measures you have undertaken to;
 - i. Assess the adequacy of the security of personal data held on the accounts (in the event that more than one platform is in use, please provide details for each such platform);
 - ii. Identify that persons using the platforms are who they purport to be;
 - iii. Ensure that accounts are only used by the person whom owns the account;
 - iv. Ensure that accounts are protected from unauthorised or unlawful access;
 - v. Ensure the security of data in transit between official Department platforms and the accounts;
 - vi. Ensure the set-up, deletion and general use of such accounts provides adequate security and protection of the data contained within them (for example, the adequacy of arrangements for the back-up of data; the prevention of automatic sharing with other aspects of an platforms' services etc);
 - vii. Provide for the restoration, availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - viii. Explain your processes for the regular testing, assessment and evaluation of the effectiveness of any technical and

organisational measures you have in place for ensuring the security of the processing;

- ix. Provide any other information you have which is pertinent to the ongoing confidentiality, integrity, availability and resilience of processing undertaken on such platforms.

Data Protection Impact Assessments (Article 35)

9. Please also explain whether:

- i. A Data Protection Impact Assessment was completed in relation to the use of such accounts, and if so provide a copy.

Purpose Limitation, accuracy and retention (Articles 5 (1) (b), (c) and (d))

10. Please explain how the Department ensures that any personal data held on the accounts is collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

11. Please explain how the Department ensures that personal data held on the accounts is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

12. Please explain how the Department ensures that personal data held on accounts is accurate and, where necessary, kept up to date.

Records of Processing Activities (Article 30)

13. In the event that such accounts are held, please explain how this is captured within the Department's Records of Processing Activities.

Data subject rights (Articles 12-22)

14. Please explain how the Department ensures that data subjects' access rights are upheld in relation to personal data held on the accounts.

Annex 2

THE DATA PROTECTION ACT 2018 (PART 6, SECTION 162)

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162 of the DPA gives any person upon whom an Information Notice has been served a right of appeal to the Tribunal against the Notice.
2. If you decide to appeal and if the Tribunal considers:-

(a) that the notice or decision against which the appeal is brought is not in accordance with the law; or

(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

the Tribunal must allow the appeal or substitute such other decision as could have been made by the Commissioner.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

General Regulatory Chamber
HM Courts and Tribunals Service
PO Box 9300
Leicester
LE1 8DJ

Telephone: 0203 936 8963
Email: grc@justice.gov.uk

a) The notice of appeal should be received by the Tribunal within 28 days of the date that the notice was sent.

b) If your notice of appeal is late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

- a) your name and address/name and address of your representative (if any);
- b) an address where documents may be sent or delivered to you;
- c) the name and address of the Information Commissioner;
- d) details of the decision to which the proceedings relate;
- e) the result that you are seeking;
- f) the grounds on which you rely;
- g) you must provide with the notice of appeal a copy of the assessment notice;
- h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and the Tribunal (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).

Annex 3

THE DATA PROTECTION ACT 2018 (PART 6, SECTION 143)

INFORMATION NOTICES – FURTHER STATUTORY PROVISIONS

Section 143 of the DPA materially states:

(1) The Commissioner may not give an information notice with respect to the processing of personal data for the special purposes unless—

(a) a determination under section 174 with respect to the data or the processing has taken effect, or

(b) the Commissioner—

(i) has reasonable grounds for suspecting that such a determination could be made, and

(ii) the information is required for the purposes of making such a determination.

(2) An information notice does not require a person to give the Commissioner information to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

(3) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—

(a) between a professional legal adviser and the adviser's client, and

(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.

(4) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—

(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,

(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and

(c) for the purposes of such proceedings.

(5) In subsections (3) and (4), references to the client of a professional legal adviser include references to a person acting on behalf of the client.

(6) An information notice does not require a person to provide the Commissioner with information if doing so would, by revealing evidence of the commission of an offence expose the person to proceedings for that offence.

(7) The reference to an offence in subsection (6) does not include an offence under—

(a) this Act;

(b) section 5 of the Perjury Act 1911 (false statements made otherwise than on oath);

(c) section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false statements made otherwise than on oath);

(d) Article 10 of the Perjury (Northern Ireland) Order 1979 (S.I. 1979/1714 (N.I. 19)) (false statutory declarations and other false unsworn statements).

(8) An oral or written statement provided by a person in response to an information notice may not be used in evidence against that person on a prosecution for an offence under this Act (other than an offence under section 144) unless in the proceedings—

(a) in giving evidence the person provides information inconsistent with the statement, and

(b) evidence relating to the statement is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(9) In subsection (6), in relation to an information notice given to a representative of a controller or processor designated under Article 27 of the UK GDPR, the reference to the person providing the information being exposed to proceedings for an offence includes a reference to the controller or processor being exposed to such proceedings.