Information Commissioner's Office

For information on how we process
personal data visit www.ico.org.uk/privacy-notice

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

DATA PROTECTION ACT 2018
(PART 6, SECTION 149)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

To: Her Majesty's Revenue and Customs

Of: 100 Parliament Square, London SWIA 2BQ

1. Her Majesty's Revenue and Customs ("HMRC") is a "data controller" as variously defined in sections 3(6), 5 and of the Data Protection Act 2018 ("the DPA") and Article 4(7) of the General Data Protection Regulation ("the GDPR"). HRMC is the tax, payments and customs authority of the United Kingdom. It processes personal data in the course of carrying out its functions.

2. The Information Commissioner ("the Commissioner") has decided to issue HMRC with an Enforcement Notice under section 149 DPA. The Notice is in relation to contraventions of the data protection principles set out in Article 5 GDPR. This Notice is accordingly issued under section 149(2)(a) DPA.

3. This Notice explains the Commissioner's decision.

Legal framework for this Notice

4. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.

5. Section 149 DPA materially provides:

"(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or

(b) to refrain from taking steps specified in the notice,

or both (and see also sections 150 and 151).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international

organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

...

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure."

6. Section 150 DPA materially provides:

"(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—

(a) to impose a ban relating to all processing of personal data, or

(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).”

7. Article 4 GDPR contains definitions of relevant terms. Along with the definition of personal data and controller, Article 4(14) defines "biometric data":

"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"

8. The data protection principles are now set out in Article 5(1) GDPR. Compliance with the principles is the responsibility of the controller: Article 5(2). The first principle ("DPP1") is provided for in Article 5(1)(a):

"Personal data shall be...processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".

9. For processing to be lawful under DPP1, processing must be in accordance with one of the bases set out in Article 6 GDPR, relevantly including:

"1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

..."

10. Further, to be lawful under DPP1, when the processing relates to special categories of personal data, it must be in accordance with Article 9 GDPR, which provides:

"1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

..."

11. Chapter III of the GDPR makes provision for the rights afforded to data subjects. These include the rights of subject access, rectification, erasure and restriction of processing.

HMRC's processing of Personal Data

12. The Commissioner's investigation into HMRC has focussed on its use of voice authentication ('Voice ID') for customer verification on some of its helplines since January 2017. The Commissioner's understanding of HMRC's processing and her findings below are based primarily on the information she has received during her investigation following a complaint by 'Big Brother Watch' into HMRC's conduct.

13. HMRC rolled out its Voice ID service in January 2017. It has enrolled around 7 million customers on this service.

14. The Voice ID service authenticates customers when they call HMRC's helplines through their voice. The characteristics of a person's voice constitute biometric data. HMRC processes this biometric data for the purpose of uniquely identifying natural persons when they call its helplines.

15. HMRC collected this biometric data when customers called some of its helplines. When they passed the standard (i.e. non-Voice ID) verification process they were given some information about the Voice ID service. As part of the initial complaint, Big Brother Watch shared two call transcripts detailing the experience of customers calling the HMRC helplines. These show that customers were informed via an automated recording that HMRC was introducing a 'quicker and more secure' means of verifying identification. The benefits of the system and how Voice ID works were explained, although the recording did not give details of where customers could find further information. The automated

recording did not inform customers that they did not have to sign up to the service. Customers were asked to repeat, "my voice is my password", and there was no clear option for callers who did not wish to register.

16. HMRC collected this biometric data before it published a Voice ID-specific privacy notice on 27 July 2018 and prior to the week of 8 October 2018 when it made further changes to the automated recording and options were presented to the customers.

17. HMRC has endeavoured to contact the customers whose biometric data it collected before it made these changes. The latest figures provided to the Commissioner (which HMRC says are correct as of 4 March 2019) indicate that roughly 20% of the 7 million customers whose biometric data was collected have responded to HMRC's subsequent contact. Of these:

    a. 995,938 customers provided consent for HMRC to continuing processing their data; and

    b. 260,551 customers withheld consent.

18. HMRC has informed the Commissioner that it has deleted the biometric data of 156,360 customers who withheld consent as at 5 January 2019. HMRC has confirmed that it is able to identify the remaining data of roughly 5.5 million customers for which it does not have explicit consent. It has also shown that it is able to delete this data.

The Contravention

19. In the circumstances, the Commissioner is satisfied that HMRC has committed the following contravention of the GDPR.

Lawful Processing: DPP1

20. HMRC has contravened DPP1 in that it has and continues to process personal data by collecting, retaining and using biometric data through its Voice ID service, without having a lawful basis for so doing under Articles 6 and 9.

21. Under Article 6(1), processing is only lawful if it is on one of the listed bases. None of these exist in this case. HMRC cannot rely on the customers having given consent (Article 6(1)(a)) as the automated recording failed to obtain adequate consent: the recording failed to give customers sufficient information on how their biometric data would be processed and failed to give them an opportunity to give or withhold consent to such processing.

22. Further, under Article 9, processing of special categories of personal data is prohibited unless at least one of the conditions in Article 9(2) is satisfied. The biometric data processed by HMRC is special category data within the meaning of Article 9(1). None of the conditions in Article 9(2) is satisfied. HMRC cannot rely on Article 9(2)(a), the only potentially relevant condition, as the customers did not provide explicit consent. The automated recording failed to obtain explicit consent for the same reasons that it failed to obtain adequate consent for the purposes of Article 6.

23. In the absence of a basis for processing under Article 6 and a condition under Article 9, the retention of this personal data is unlawful.

Issue of the Notice

24. The Commissioner considers that the contravention is a significant one which warrant enforcement action. Her reasons for this conclusion include that:

- An extremely large number of data subjects are affected.
- HMRC collected this personal data in circumstances where there was a significant imbalance of power between it and its customers. It did not explain to customers how they could decline to participate in the Voice ID system. It also did not explain that customers would not suffer a detrimental impact if it declined to participate.
- The imbalance of power may still be a factor in the number of customers who have not withheld consent, especially where customers rely on HMRC for benefit purposes.
- HMRC appears to have given little or no consideration to the data protection principles when rolling out the Voice ID service.

25. The Commissioner considered, as she is required to do under section 150(2) DPA when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner does not conclude that damage or distress is likely in the present

context. However, data subjects are likely to be concerned about the processing of their personal data in the manner set out above, in circumstances where the full nature of that processing is not clearly drawn to their attention and they were not given an opportunity to provide or withhold consent at the time their data was collected.

26. Furthermore, and in any event, the Commissioner considers that compliance with the principles in Article 6 and Article 9 to be a matter of central importance to data protection law. Even if a failure to comply has not, or is not likely, to cause any person damage or distress, the issue of this Enforcement Notice to compel compliance would nonetheless be an appropriate exercise of the Commissioner's enforcement powers.

27. The Commissioner has also had regard to HMRC's attempts retrospectively to obtain explicit consent for the processing. Though these efforts are welcome (and have resulted in 995,938 customers providing consent) they do not make it lawful for HMRC to continue processing the remaining personal data of roughly 5.5 million customers.

28. Having regard to the significant nature of the contravention, the scale of the personal data being processed and the context in which it is processed, the Commissioner considers that this Enforcement Notice is the proportionate regulatory step to bring HMRC into compliance.

29. In view of the above, and in exercise of her powers under section 149(2)(a) DPA, the Commissioner requires HMRC to take the

steps specified in Annex 1 within 28 days of this Notice.

Consequences of failing to comply with this Enforcement Notice

30. If a person fails to comply with an Enforcement Notice the Commissioner may serve a penalty notice on that person under section 155(1)(b) DPA requiring payment of an amount up to 20 million Euros, or 4% of an undertaking's total annual worldwide turnover whichever is the higher.

ico.
Information Commissioner's Office

Consequences of failing to comply with this Enforcement Notice

31. By virtue of section 162(1)(c) DPA, there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights). If an appeal is brought this Notice need not be complied with pending determination or withdrawal of that appeal. Information about the appeals process may be obtained from:

First-tier Tribunal (Information Rights)
GRC & GRP Tribunals
PO Box 9300
Leicester
LE1 8DJ

Tel: 0300 1234504
Fax: 0870 739 5836
Email: GRC@hmcts.gsi.gov.uk
Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

32. Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Notice is sent.

Dated the 9th day of May 2019

Signed: ....[redacted]

Steve Wood
Deputy Commissioner (Executive Director – Policy)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

TERMS OF THE ENFORCEMENT NOTICE

HMRC shall, within 28 days following the date of this Notice (and following the permissible time for appealing this notice):

- Delete all of the biometric data held under the Voice ID system for which it does not have explicit consent.

- Require its suppliers who operate, manage or are involved in the Voice ID system to delete all the biometric data they process under the Voice ID system for which it does not have explicit consent.