Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 2797 Email JCHR@parliament.uk Website www.parliament.uk

From Rt Hon Harriet Harman MP, Chair

Rt Hon Matt Hancock MP
Secretary of State for Health and Social Care
Department of Health and Social Care
39 Victoria Street
London
SW1H 0EU

7 May 2020

Dear Matt,

Thank you for your letter of 5th May and we are grateful for your assurances about privacy in the Contact Tracing App. But we note that you don't consider legislation is necessary.

We do think legislation is necessary as we set out in our report, Human Rights and the Government's Response to Covid-19: Digital Contact Tracing, published 7th May.

The current law is an unsatisfactory mishmash spread across the GDPR, the Data Protection Act 2018, Article 8 European Convention on Human Rights and caselaw on the right to privacy.

That, as our report last year affirmed, has already proved inadequate to protect the individual from misuse of their data. But the Contact Tracing App is a more significant data collection mechanism that anything envisaged hereto.

The assurances you give in your letter would be better in bespoke legislation and to assist we have produced a draft Bill which I attach herewith.

It is not our intention to delay the roll out of the Contact Tracing App due in the next couple of weeks after the Isle of Wight pilot. But we believe that Parliament could quickly and consensually pass this law. It has already done that in giving the Government the powers it needs for tackling this pandemic

We look forward to your reply and to your agreement that you will adopt this Bill and present it to parliament.

Yours sincerely

Harriet Harman

Rt Hon Harriet Harman MP
Chair of the Joint Committee on Human Rights

A

B I L L

TO

Make provision for the regulation of the processing of information in respect of contact tracing for Covid-19; and for connected purposes.

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Interpretation

1 Contact tracing

For the purpose of this Act—

(a) "digital contact tracing" means the use of communications technology to trace individuals who have been in contact with individuals infected with coronavirus;

(b) "digital contact tracing data" means personal data obtained through digital contact tracing;

(c) "digital contact tracing system" means a system designed or used for the processing of digital contact tracing data; and

(d) "contact tracing app" means a mobile phone application designed or used to facilitate digital contact tracing.

2 Permitted contact tracing purposes

For the purposes of this Act the "permitted contact tracing purposes" means—

(a) protecting the health of individuals who are or may become infected with Coronavirus;

(b) preventing or controlling the spread of Coronavirus.

3 Mobile device

In this Act "mobile device" means—

(a) a mobile telephone, and

(b) any other communications device that is designed to be portable.

4 Other expressions

Definitions in the following Acts apply for the purposes of this Act—

(a) the Coronavirus Act 2020; and

(b) the Data Protection Act 2018.

Digital Contact Tracing Human Rights Commissioner

5 Appointment

(1) The Secretary of State must appoint a person as the Digital Contact Tracing Human Rights Commissioner ("the Commissioner").

(2) The provisions of the Data Protection Act 2018 about the powers and proceedings of the Information Commissioner apply (with any necessary modifications) to the Commissioner.

(3) The first appointment under this section must be made before the end of the period of 28 days beginning with the date of Royal Assent.

6 Functions: review

The Commissioner must review—

(a) the application to digital contact tracing of the law relating to privacy, data protection and human rights;

(b) the processing of digital contact tracing data by Ministers of the Crown and other public authorities;

(c) the security of digital contact tracing systems;

(d) risks associated with the identification of individuals to which digital contact tracing data relates; and

(e) whether digital contact tracing remains necessary and proportionate for digital contact tracing purposes.

7 Functions: complaints

(1) The Commissioner must establish a system for receiving complaints about digital contact tracing.

(2) The provisions of the Data Protection Act 2018 apply to complaints to the Commissioner as to complaints by data subjects under section 165 of that Act; and for that purpose—

(a) a reference to infringement is a reference to infringement of this Act, and

(b) the provisions apply with any other necessary modifications.

8 Inspections

(1) Without prejudice to the generality of section 5(3), the provisions of the Data Protection Act 2018 relating to powers of entry and inspection apply for the purposes of this Act—

(a) as if references to the Information Commissioner were references to the Commissioner;

(b) as it references to offences under that Act were to offences under this Act; and

(c) with any other necessary modification.

Digital contact tracing data

9 Processing of digital contact tracing data

(1) It is an offence for a person who is not an authorised person to collect or process digital contact tracing data.

(2) In subsection (1) "authorised person" means—

(a) the Secretary of State; or

(b) a person specified by the Secretary of State by regulations.

(3) An authorised person may not collect or process digital contact tracing data other than for a permitted contact tracing purpose.

(4) The Secretary of State must take all reasonable steps to ensure that systems used for processing digital contact tracing data—

(a) are designed so as to process no more data than is required for the permitted contact tracing purposes; and

(b) are as secure as possible.

(5) It is an offence for a person knowingly or recklessly to re-identify de-identified digital contact tracing data.

(6) For the purpose of subsection (5) —

(a) digital contact tracing data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific individual;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).

10 Security assessments

(1) The Secretary of State must arrange for the security of digital contact tracing systems to be reviewed by the National Cyber Security Centre.

(2) A review must be carried out—

(a) during the period of 28 days beginning with the date of Royal Assent; and

(b) at least once during each succeeding period of 28 days.

(3) In this section National Cyber Security Centre means civil servants designated by the Secretary of State.

11 Collection of mobile data

Digital contact tracing data may not be collected from a mobile device unless each person who owns or operates the device has given consent.

12 Deletion of data

(1) A digital contact tracing system must comply with approved arrangements for the deletion of contact tracing data.

(2) In subsection (1) "approved arrangements" means arrangements published by the Secretary of State.

(3) Before publishing arrangements the Secretary of State must consult the Commissioner.

(4) For the purposes of subsection (3), if at the relevant time the Commissioner has not yet been appointed, the Secretary of State must consult the Information Commissioner

(5) Approved arrangements must—

(a) make separate provision requiring the automatic deletion of digital contact tracing data from mobile devices as soon as is practicable;

(b) provide that no digital contact tracing data is shared from a mobile device unless the person has specifically consented to upload their digital contact tracing data;

(c) ensure that any digital contact tracing data held by an authorised person is anonymised as soon as is practicable after it is obtained;

(d) ensure that digital contact tracing data held by an authorised person is deleted or anonymised as soon as it is no longer required for a permitted contact tracing purpose; and

(e) ensure that digital contact tracing data is deleted where a data subject so requests.

(6) For the purposes of subsection (5), digital contact tracing data is "anonymised" if it has been processed in such a manner that it can no longer be attributed to a specific individual either alone or in conjunction with other data.

13 Review

(1) The Secretary of State must review the need for the digital contact tracing.

(2) A review must be carried out—

(a) during the period of 21 days beginning with the date of Royal Assent; and

(b) at least once during each succeeding period of 21 days.

(3) A review must consider—

(a) whether digital contact tracing has been effective in achieving the permitted contact tracing purposes;

(b) potential for discrimination contrary to the Equality Act 2010;

(c) potential for breaches of Convention rights (within the meaning of the Human Rights Act 1998);

(d) any complaints upheld under this Act; and

(e) the security of contact tracing data.

(4) As soon as possible after conducting a review the Secretary of State must—

(a) publish a review, and

(b) lay it before Parliament.

(5) If, at any stage the Secretary of State concludes that the processing of contact tracing data is no longer necessary for or proportionate to the purposes set out in section 3 of this Act, then he must immediately—

(a) direct any authorised person to stop processing contact tracing data, and

(b) direct any authorised person to delete any contact tracing data which that person retains.

Obligation to publish information and documents

14 Transparency

(1) The Secretary of State must publish on the gov.uk website the following:

(a) Any Data Protection Impact Assessments required of any data controller under Article 35 of the General Data Protection Regulation (GDPR) relating to digital contact tracing;

(b) Information relating to the design and security of the contact tracing app;

(c) Minutes of meetings and reports by the Contact Tracing Ethics Advisory Board.

(2) The items referred to subsection (1) must be published as soon as reasonably practicable after they are received by Secretary of State and in any event no more than 14 days thereafter.

Offences

15 Penalties for offences

(1) A person who commits an offence under section 9 is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) a conviction on indictment, to a fine.

Final Provisions

16 Regulations

(1) Regulations under this Act:

(a) may make provision generally or only for specified purposes;

(b) may make different provision for different purposes;

(c) may include incidental, consequential or transitional provision; and

(d) shall be made by statutory instrument.

(2) A statutory instrument containing regulations under this Act shall be subject to annulment in pursuance of a resolution of either House of Parliament.

17 Commencement

This Act comes into force on the day on which this Act is passed.

18 Extent

This Act extends to England and Wales, Scotland and Northern Ireland.

18 Short Title

This Act may be cited as the Contact Tracing (Data Protection) Bill 2020.