

BIG BROTHER WATCH

Big Brother Watch Briefing on The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020 for the House of Lords

October 2020

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Direct line: 020 8075 8478

Email: silkie.carlo@bigbrotherwatch.org.uk

Madeleine Stone

Legal and Policy Officer

Direct line: 020 8075 8479

Email: madeleine.stone@bigbrotherwatch.org.uk

INTRODUCTION

We welcome the opportunity to provide this briefing to the House of Lords ahead of the motion on The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020 on 7th October 2020.

In particular, we welcome the opportunity to provide this briefing due to the severity of our concerns arising from these Regulations. Big Brother Watch and Open Rights Group have instructed data rights agency AWO to ask the Secretary of State to urgently clarify aspects of these Regulations that are unclear and unworkable; to explain the stated failure to conduct obligatory impact assessments; and to provide transparency of the operation of the Regulations as required by data protection laws. We sought an urgent response to these basic questions. However, the Secretary of State was unable to provide this basic information and instead sought 14 days to respond – a deadline that has now been missed without explanation.

We are now considering further action.

RECOMMENDATION

- **Peers should vote against these Regulations, which are excessive, intrusive, punitive, potentially discriminatory and raise serious questions of compatibility with data and privacy laws.**

Rule by diktat

These Regulations were laid before Parliament on 17th September and came partially into force on 18th September. The Regulations came fully into force on 24th September, when the NHS Covid-19 app was released.

This debate in the Lords is taking place 2.5 weeks after this extraordinary Regulation was imposed on thousands of businesses across the country, affecting the entire population of England. No debate is yet scheduled for the Commons.

The impact of this legal change cannot be understated. These Regulations introduce the potential for the mass recording of citizens' movements by an array of ill-equipped, over-stretched businesses.

It is only by closely following Government websites that a business would even become aware of the new obligations and financial penalties. These Regulations were published just hours before coming into force and the communication of precisely what they entail has been minimal.

Indeed, the Parliamentary Estate has been in breach of the Regulations. As recently as 30th September, Big Brother Watch found that contact details were not being collected at the parliamentary bars and canteens; QR codes were not being displayed and scanning was not being checked; and consequently, entry was not refused to those who did not comply,¹ all in breach of the present Regulations. Despite claims to the contrary, these Regulations do not exempt Parliament from the law and nor do they exempt workplace canteens if there is a wider test and trace system in the workplace.

Duration

This Regulation expires after 12 months² and the Health Secretary must review the necessity of the Regulation after six months (i.e. before 24th March 2021).

Affected premises

The Regulations apply to venues in hospitality, the tourism and leisure industry, close contact services and local authority facilities. This includes:

- pubs
- bars
- restaurants
- workplace canteens
- amusement arcades
- art fairs
- museums and galleries
- public libraries
- youth and community centres-institutes

1 Parliament faces £1,000 fine for not asking customers to give Covid-19 tracing contact details – Matt Dathan, The Sun, 30th September 2020: <https://www.thesun.co.uk/news/12803767/parliament-1000-fine-customers-contact-details/>

2 The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020, Reg. 21

- village halls
- betting and bingo halls and casinos
- sports club, leisure centres and stadia
- outdoor swimming pools
- heritage locations open to the public
- hotels and any commercial guest accommodation including B&Bs, boats, campsites, caravans, chalets, guest houses, holiday parks, hostels, motels, pubs, sleeper trains and yurts
- music recording studios open for public hire or other public use
- barbers and hairdressers
- beauticians, wellness treatment providers, massage therapists, nail bars/salons
- piercing services and tattooists
- dress fitters, tailors and fashion designers;

In venues with communal or open-plan dining areas such as food courts, the responsibility lies with the legal owner.³ It is unclear how the obligations in this Regulation could be practically fulfilled by food court owners.

Manual data collection

The Regulations require this wide range of premises to request contact details from individuals, including their name, phone number (or email address or postal address if this is unavailable) and the date and time⁴ in order to enter the premises.⁵ Where contact details are collected from an individual who is likely to interact with only one staff member, that staff member's name must be recorded as well.⁶

If a group of people wish to enter, the premises must either collect every individual's contact details or the details of a single member of the group. If the group lawfully exceeds six people, the premises must request, as a minimum, the contact details of one person per each sub-group of six.

Only children under the age of 16 and people unable to provide details owing to a disability or health problem are exempt.⁷ Furthermore, visits for post, orders or food collection are exempt (as well as visits by emergency responders and police).⁸

NHS Covid-19 app and QR codes

As of 24th September, the release date of the NHS Covid-19 app, the Regulations additionally require premises to display a QR code⁹ and require anyone entering the premises to either use the app to scan the QR code and thus register their entry,¹⁰ or to provide their personal details to staff in the manual way described above.

³ Maintaining records of staff, customers and visitors to support NHS Test and Trace – Department of Health and Social Care, 18th September 2020: <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace> (accessed 6 October 2020)

⁴ The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020, Reg. 10

⁵ The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020, Reg. 7(2)

⁶ Reg. 11

⁷ Reg. 7(4)

⁸ Reg. 9(2)

⁹ Reg. 6

¹⁰ Reg. 6(2), 7(3)

Government guidance states that, should an individual use the NHS app to scan a QR code in order to gain entry, “a venue should check their phone screen” to ensure they have actually “checked in”.¹¹ As such, this scheme gives license to thousands of people to demand to check the personal phones of individuals. Many people will rightly find this intrusive, and many business owners and employees will find this burden onerous.

Big Brother Watch has, along with many other NGOs and technologists, argued throughout this pandemic that any contact tracing app must be strictly voluntary, non-punitive and non-discriminatory. Trust in contact tracing should be earned; it cannot be compelled through exclusion and punishment. However, the Government is increasingly relying on criminal sanctions to manage public health instead of trusting citizens to act responsibly with free will.

The legal requirement for venues to ensure the app is used or personal details are given as a condition of entry makes use of the app de facto compulsory in order to engage in everyday life; it discriminates against people who cannot use the app, who are likely to be older people or poorer people who do not have smart phones with the latest software; and it punishes those who do not want to give their personal details by refusing their entry to everyday businesses.

We are aware of several reports of premises that now require use of the NHS app as a condition of entry. This is likely due to businesses’ self-awareness that they cannot become legally compliant data controllers overnight and their caution to avoid liability. Government guidance advises against this practice¹² – but it is an obvious consequence of their punitive legislative approach to the collection of personal details. This is one of many reasons these Regulations should be repealed.

Data retention

The premises must securely retain this personal data for 21 days and destroy the data after that period, “unless there is another basis outside these Regulations on which the details may lawfully be retained.”¹³ Moreover, the data must be retained and secured in line with the Data Protection Act 2018 and GDPR. Furthermore, every affected business will have to register as a data controller with the Information Commissioner’s Office and pay the relevant fee.

However, it is unrealistic to expect businesses, especially small businesses, to become fully-compliant data controllers overnight. As a result, thousands of customers’ data is highly likely at risk.

Furthermore, it is important to note that this data may reveal sensitive personal information, such as their sexuality, and thus requires a particularly high level of protection.

We are already aware of cases where contact details collected for the purposes of contact tracing have been retained and used for unwanted marketing, and even misused by staff to send unsolicited personal messages¹⁴ – an problem which overwhelmingly affects women and girls. We have notified the ICO of

11 Maintaining records of staff, customers and visitors to support NHS Test and Trace – Department of Health and Social Care, 18th September 2020: <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace> (accessed 6 October 2020)

12 Ibid.

13 Reg. 13

14 For example: Track and trace: Woman gets ‘creepy’ text from restaurant manager pretending to be from NHS contact tracing – Claudia Tanner, iNews, 1 October 2020: <https://inews.co.uk/news/real-life/track-and-trace-nhs-contact-tracing-restaurant-manager-text-woman-671591>

this in the course of acting for a young woman who was harassed by a male bartender after providing her details on request for contact tracing. The business denied any liability and the ICO did not intervene or reply to us.

It is wholly disproportionate to force every person in England to expose themselves to this risk, against their will, in order to enter everyday premises.

The Department of Health and Social Care has provided a template privacy notice,¹⁵ as all affected businesses are expected to provide a legally-compliant privacy notice at the point of data collection. The template, which is incomplete, is 916 words long and takes approximately 8 minutes to read. It is clearly unrealistic that customers will be able to read such notices on a mass scale.

Data disclosure

Premises must provide the data to the Secretary of State or a public health officer on request.¹⁶ The Secretary of State may request the data where they consider it necessary for contact tracing.¹⁷

It is unclear what persons, agencies, companies or other organisations may also receive or process the data transferred to the Secretary of State or public health officers. Article 13 GDPR requires that individuals are informed of “the recipients or categories of recipients of the personal data” at the point of data collection. However, even the most data protection compliant businesses cannot possibly do this if the Secretary of State will not readily disclose the recipients.

Requirement to refuse entry

The Regulations impose on hospitality venues – namely pubs, bars, cafes and workplace canteens – a legal requirement to “take all reasonable steps to prevent entry” to anyone who does not either scan the QR code or provide their full and accurate personal details.¹⁸ The accompanying guidance suggests that organisations “follow [their] own security procedures” if an individual becomes “unruly”, or even call the police “if you feel the individual poses a risk to yourself or others.”¹⁹

This extraordinary legal requirement seeks to deputise businesses as agents of draconian state rules, requiring hospitality and leisure staff to deny physical entry to premises to members of the public. It is wholly disproportionate, inappropriate, and likely to seed conflict.

Penalties

Venues that fail to comply with these requirements commit an offence and are liable for prosecution²⁰ or a fine starting at £1,000 and going up to £4,000,²¹ which may be issued by a police officer, PCSO, council

15 Annex B – Template privacy notice; Maintaining records of staff, customers and visitors to support NHS Test and Trace – Department of Health and Social Care, 18th September 2020: <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace> (accessed 6 October 2020)

16 Reg. 15

17 Reg. 14

18 Reg.16

19 Maintaining records of staff, customers and visitors to support NHS Test and Trace – Department of Health and Social Care, 18th September 2020: <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace> (accessed 6 October 2020)

20 Reg. 19

21 Reg. 18

official or other authorised person.²² At a time when many businesses in the hospitality and leisure sector are struggling, in debt, closing or going bankrupt, these punitive fines backing unrealistic and extremist measures are harmful and prohibitive.

Privacy questions

The explanatory note to the Regulations states “No regulatory impact assessment has been provided for these Regulations.” A Data Protection Impact Assessment (DPIA) has been published for the NHS Covid-19 app²³ but it is not clear whether the DPIA or Equality Impact Assessment has been conducted for the Regulations, or the NHS Test and Trace system as a whole. These assessments are legally required prior to the roll-out of the scheme. **Their absence throws the legal compliance of the system into question.**

We instructed lawyers to urgently write to the Secretary of State on this point, on 23rd September. As of 6th October, we are yet to receive a reply. We are now considering further action.

²² Reg. 18(11)(a)

²³ NHS COVID-19 app: data protection impact assessment – updated 1st October 2020