A W O

RECIPIENT
Matthew Hancock
Secretary of State
Department of Health and Social Care
39 Victoria Street
London
SW1H 0EU

By email

LETTTER BEFORE CLAIM

DATE
1st of July 2020

OUR REF: RAN/00023

SENDER
Ravi Naik
Director
2 John Street, London.
WC1N 2ES

+44 (0) 0123 456 789
ravi@awo.legal

www.awo.legal

Dear Secretary of State
Open Rights Group

We are instructed by Open Rights Group ("ORG"), a UK-based digital campaigning organisation working to protect rights to privacy and free speech online.

We write further to our correspondence concerning the NHS Test and Trace Programme ("the Programme") with Ms Karen Perry, Private Secretary to David Williams CB, Second Permanent Secretary of the Department of Health and Social Care ("DHSC") in June 2020.

The Programme, which was deployed on 28 May 2020 as part of the UK's response to COVID-19, involves the mass collection, analysis and storage of personal data (and sensitive personal data by DHSC and other public and private third parties. This data includes the names, contact details and data concerning the health of thousands of the UK population. An indication of the scale of the data processed pursuant to the Programme was given by the Prime Minister, Boris Johnson, who at Prime Minister's Questions on 24 June 2020, stated that over 87,000 individuals had already been contacted by the Programme.

However, despite the significant risks to the privacy rights of the hundreds of thousands (if not millions) of individuals in the UK whose personal data has been or will be processed through the Programme, our clients understand that processing of personal data pursuant to the Programme began (and continues to take place) without any, or any sufficient, assessment of the risks by a Data Protection Impact Assessment ("DPIA").

We consider that processing of personal data under the Programme has been conducted in breach of the requirements of the Data Protection Act 2018 ("DPA") and Article 35 of the General Data Protection Regulation ("GDPR").

We ask that the DHSC reconsider its position that the DPIA(s) that have been undertaken (in relation to an entirely separate system) addresses the type of widescale processing operations envisaged by the Programme. If the DHSC is unwilling to do so, ORG will bring a judicial review claim seeking appropriate declarations and other relief in respect of this.

Given the history of the pre-action correspondence in this matter, and the fact that the processing pursuant to the Programme continues to operate without a DPIA, we request a response within 7 days of receipt of this letter. We are instructed to issue proceedings without delay in the absence of a satisfactory response.

1. The Proposed Claimant & Defendant

Should the commencement of proceedings become necessary, the Proposed Claimant in this matter is ORG, who can be contacted via this firm. You are already in receipt of our clients' authority to act.

The Proposed Defendant is the DHSC.

2. The Proposed Claimant's legal representative

ORG's representative is Mr Ravi Naik of our offices. Mr Naik's contact details are at the top of this letter.

The reference number for this case is RAN/00023. Please use this reference in any correspondence. Please also provide your reference number for this matter.

3. Background

The NHS, through Public Health England ('PHE'), launched the Programme on 28 May 2020. On the same date, a spokesperson for PHE, Julia Thompson, stated that a DPIA had not been conducted for the Programme. Ms Thompson was reported to have stated that PHE were "preparing a data protection impact assessment for the NHS Test and Trace system" which it "expects to publish this shortly."[1]

On 2 June 2020, our clients requested further information on the rapid deployment of the Programme and expressed concerns regarding the failure to conduct a DPIA prior to the processing of data under the Programme. Our letter asked four questions concerning the DPIA, including whether it was correct (as suggested by Ms Thompson) that no DPIA had been conducted prior to the deployment of the Programme and, if so, why. We sought an answer by 4 June 2020.

No response was received by 4 June 2020. Chasing emails were sent on 5 and 8 June 2020. On 10 June 2020, Ms Perry emailed to say the DHSC "commit[ted] to" replying by 16 June 2020. No response was received by that date. Rather, on 16 June 2020, Ms Perry stated that DHSC "will reply" by 22 June 2020. In response to that communication, our client then asked a single

[1] https://www.politico.eu/article/uk-test-trace-privacy-data-impact-assessement/

question about the DPIA: Was test and trace deployed without a DPIA having been conducted?

In response, Ms Perry stated (sic):

> *"there were DPIAs - and accompanying privacy notices - undertaken for both the testing and contract tracing advisory service (CTAS) aspects of the programme, which augment pre-existing assessments regarding public health tracing functions."*

Ms Perry further confirmed that "We will respond substantively to your remaining detailed questions by close on Monday 22nd June."

This was the first time that the CTAS system had been mentioned in correspondence from the DHSC. On 18 June 2020, our clients sought clarification of that system and how it relates to the Programme. On 19 June 2020, Ms Perry replied as follows:

> *"The Test & Trace Programme consists of both contact tracing elements and testing. The document to which you have provided the link refers to the NHS Test and Trace contact tracing service and sets out what data is collected and how that data is used by the groups listed in support of our overall contact tracing effort. The testing element is separate and so as well as the privacy notice for CTAS, we would also refer you to these documents:*
>
> *1. https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information*
>
> *2. https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information*
>
> *which refer to the testing element. Accordingly, we can confirm that separate DPIAs and PNs were undertaken for separate contact tracing and testing elements of the Programme as previously stated in our response on Wednesday . These DPIAs and PNs were in place by 28 May – and we continue to review in light of the dynamic nature of the Programme."*

On 19 June 2020, a detailed email of response was sent to Ms Perry seeking to clarify the relationship between CTAS and the Programme. In particular, we sought clarification of the following matters:

i. whether the CTAS system, which appeared from publicly available material to be the web-portal through which manual contract tracers logged in rather than the Programme as a whole, covered the types of processing envisaged by the Programme;
ii. what aspects of the Programme were covered by the DPIA conducted for the CTAS system;
iii. whether the information provided by Ms Thompson was incorrect.

A response to that email was sought in the substantive response due on 22 June 2020. No response was received by that date. Following further chasing emails, Ms Perry sent an email at 20:39 on 23 June 2020. The pertinent part of that email stated

"We write further to your letter of 6 June 2020 and respond accordingly.

A. Test, Trace and Isolate

You have asked about the completion of a Data Protection Impact Assessment prior to the launch of for the Test and Trace Programme on 28 May 2020. In relation to that we refer to my emails dated 17 and 19 June 2020. Those emails set out the DPIAs that had been undertaken and which continue to be updated in respect of the elements of Test and Trace Programme as at that date. We would point out that Article 35 of the GDPR is not prescriptive as to the form that any DPIA must take. Therefore, it is not a breach of the GDPR for there to have been a number of DPIAs instead of a single unified DPIA. The proper focus instead is on whether those DPIAs (single or multiple) identify the relevant risks presented by the Programme and assess their impacts in accordance with the GDPR.

We seek to reassure you that we are committed to working closely with the ICO on all aspects of the Test and Trace programme and wish to reaffirm here our commitment to ensuring we comply with all the relevant privacy and legal standards we are bound by."

On 25 June 2020, our clients sought further direct clarification of whether the CTAS system was the same system as the Programme, as this information had not been provided, despite repeated requests for the same.

On 26 June 2020, Ms Perry responded to confirm that:

"CTAS is also known as the NHS Test & Trace website. It is the website used by the NHS Test & Trace service to identify and trace the contacts of people who test positive for coronavirus."

We understand Ms Perry to have confirmed that the CTAS system is a website, which is part of the Programme as the online portal for the contact tracers, but not the Programme as a whole.

4. Relevant Legal Framework

The requirement to conduct a DPIA is contained in Article 35 of the GDPR, which provides (in relevant part):

"1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. ...

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects

concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale. ...

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. ...

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations."

Recital 91 provides that a DPIA is necessary in respect of large-scale processing operations.

The Article 29 Data Protection Working Party's (the 'WP') Guidelines on DPIA (October 2017)[2], which have been endorsed by the European Data Protection Board, give examples of "high risk" processing operations, including the processing of sensitive data or data of a highly personal nature; data processed on a large scale and where processing involves the use of innovative or new technological solutions. This is consistent with the ICO's "*Examples of processing 'likely to result in high risk'*"[3], which include "Innovative technology", "Tracking" and "Large-scale processing".

The WP Guidelines describe the circumstances in which revision of an existing DPIA would be required:

"[A] DPIA could be required after a change of the risks resulting from the processing operations, for example because a new technology has come into use or because personal data is being used for a different purpose. Data processing operations can evolve quickly, and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a

[2] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (as approved by the EDPB)

[3] ICO, 'Examples of processing 'likely to result in high risk'' < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>

changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned."

The WP Guidelines note that a revised DPIA may be required where there is a change in the "data collected, purposes, functionalities, personal data processed, recipients, data combinations, risks (supporting assets, risk sources, potential impacts, threats etc.), security measures and international transfers." The ICO also states that a DPIA needs to be kept under review and may need to be repeated where there is a "substantial change to the nature, scope, context or purposes" of the processing.

In *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 672 at §148, the DPIA conducted by South Wales Police was found to satisfy the requirements of the DPA 2018 only where (i) there was a "clear narrative that explain[ed] the proposed processing" and "refer[red] to the concerns raised in respect of intrusions into privacy of members of the public"; (ii) the DPIA "specifically consider[ed] the potential for breach of article 8 rights"; and (iii) the DPIA "recognise[d] that personal data of members of the public will be processed, and identify[ed] the safeguards that are in place in terms of the duration for which any such data will be retained, the purpose for which it will be used, and so on."

5. Proposed Grounds of Judicial Review

Pursuant to Article 5(2) GDPR, the burden of proving compliance is on the DHSC. Our clients have made enquiries with DHSC about the DPIA conducted in relation to the processing of personal data by the Programme. The responses from DHSC failed to answer our clients' questions in a clear and comprehensible manner. We understand from DHSC's responses that the current DPIA only relates to the CTAS system and unspecified parts of the testing system, and therefore does not cover the whole of the Programme. We therefore infer that there are important aspects of the Programme which are not directly addressed in any extant DPIA.

We do not understand that there to be any dispute that:

i. A DPIA is required for any processing that "is likely to result in a high risk to the rights and freedoms of natural persons" and that the Programme presents sufficiently high risk to require a DPIA. Our letter dated 2 June 2020 explains why the processing undertaken pursuant to the Programme involves such a risk.
ii. The DPIA must be conducted prior to processing, pursuant to Article 35(1) GDPR and should have been in place prior to the deployment of the Programme.

If our understanding that these points are common ground is not correct, we ask that you let us know and provide detailed reasons for your position.

Assuming that out understanding is correct, it follows that there are two issues between the parties:

i. whether the DPIA(s) for the CTAS system and unspecified parts of the testing system involve "an assessment of the impact of the envisaged processing operations [of the Programme as a whole] on the protection of personal data" for the purposes of Article 35(1) GDPR; and

ii. whether under Article 35(11) GDPR the DPIA(s) for the CTAS system and unspecified parts of the testing system should have been reviewed or repeated because there was a change to the nature, scope, context or purposes of the processing operations envisaged under the DPIA.

We consider that the answer to the first question is "yes" and the second question is "no". We note, however, that due to the dilatory and obfuscatory nature of the responses from DHSC to our previous correspondence, and the failure to disclose the DPIA(s) conducted for the CTAS system and the testing system (despite our clients' repeated requests for the same), we only have a limited picture of what has actually been done by DHSC and the extent of their compliance with the requirements of the DPA 2018 and GDPR. Accordingly, our understanding of the position is premised on the limited information which the DHSC has provided in correspondence and what our clients are able to glean from publicly available sources. On the basis of that information, however, it would appear that the CTAS system and testing systems could only cover a few narrow parts of the Programme, and therefore would not have considered all of the processing operations undertaken in the Programme.

The DPIA(s) for CTAS and the testing system appear not to cover all of the different processing operations undertaken as part of the Programme. Accordingly, DHSC was (and is) required to either undertake a separate DPIA in respect of the Programme as a whole, or to produce a substantially revised version of the existing DPIA(s) so as to address the processing risks inherent in all of the processing operations now encompassed by the Programme. Accordingly, in order to comply with Article 35 GDPR, the DHSC must either conduct a separate DPIA in relation to the Programme or substantially review and update the existing DPIA(s) in order to ensure that the full impact of <u>all</u> of data processing operations involved in the Programme is properly assessed. In this regard, we draw particular attention to the following points:

i. *First*, the CTAS is only the web portal for the Programme. It is not the Programme and does not envisage the same processing operations as the Programme. A blog post by Duncan Selbie, the Chief Executive of PHE, on 24 April 2020 states that "PHE built a new Contact Tracing and Advisory Service, which is an online platform where people with a positive COVID-19 test result can input their history of contacts, giving the contact tracers a flying start in working out who they need to reach by email and phone."[4] This is consistent with how Ms Perry described CTAS. Likewise, the privacy notice of the testing programme relates only to "a home test or a test at a regional test site".

[4] https://publichealthmatters.blog.gov.uk/2020/04/24/duncan-selbies-friday-message-24-april-2020/

By contrast, the Programme is the integrated national system as a whole. The scope of the processing activities undertaken pursuant to the Programme is far wider and more diverse. In particular, the Programme also covers the "Trace" aspect. This includes processing of special category data, such as medical contact data (i.e. details of those individuals that individuals who have tested positive for COVID-19 have been in contact with). This does not appear to be covered by the CTAS or the testing programme.

The processing of data under the Programme therefore involves a substantial change in risk to the risks that exist under the CTAS system. In particular, there are significant differences in terms of the amount and nature of the data collected, the purpose and manner of such collection, and the uses to which the collected data are put.

ii. *Second*, the Programme involves new third party data processors and/or joint controllers. For example, the Programme involves the sharing of data with Amazon Web Services, Serco UK and the SITEL Group. Of these companies, only Amazon performs the same role between CTAS and the Programme. Serco performs a different role between the Programme and CTAS / testing, providing "facilities management for some regional test sites" for testing but providing "additional staff to call the contacts of people with COVID-19 and provide advice on self-isolation" for the Programme. SITEL have no declared involvement at all with CTAS. The WP Guidelines specifically identify a change in the recipients of personal data as an example of a circumstances which requires a new or revised DPIA is required. Accordingly, the involvement of new third party data processors and/or joint controllers is sufficient in itself to trigger the need for a new or updated DPIA pursuant to Article 35 GDPR.

iii. *Third*, CTAS and the testing system have their own privacy notice (as set out in Ms Perry's email of 19 June 2020), which differs from and is distinct from the privacy notice for the Programme. The differences between the respective privacy notices reflects the different scope, purpose and nature of the Programme and, hence, the different (and greater) risks that apply to the processing of personal data pursuant to the Programme.

iv. *Fourth*, the Programme has wider data retention structures than CTAS. For instance, the retention period as stated on the privacy notice for the Programme is 20 years[5]. The testing / CTAS systems have a retention period of 8 years. The application of a retention period which is 2.5 times longer than the retention period under the testing/CTAS system plainly represents a "change of the risk represented by processing operations" for the purposes of Article 35(1) GDPR.

v. *Fifth*, CTAS predates the Programme by a number of months. There is little publicly available information available about the CTAS system. However, we note that CTAS was referred to in a letter from the Deputy

[5] We note you have agreed to amend the period to 8 years following our clients' correspondence. However, at the time of writing this change has not been implemented.

Chief Executive of PHE as making up a single part of the developing national "approach to contact tracing", distinct from "phone-based contact tracing" involved in the Programme. That letter was dated 24 April 2020, well before the current Programme was developed. Further, at the Coronavirus briefing on 25 May 2020, Yvonne Doyle referred to CTAS being "set up … in March on a trial basis. And we're now at working to connect that, and it will connect with the various places that people will need follow up and will need support and contact tracing".

When the DPIA for CTAS and the testing programme was conducted, the wide scale of processing operations undertaken pursuant to the Programme was not contemplated. As a result, the Trace aspect has not, and could have not, been assessed in the DPIA(s) undertaken in respect of those systems. It is also apparent that "the societal context for the processing [had] changed"[6] between CTAS being operational in March and the deployment of the Programme on 28 May 2020. This is a further example of a circumstance in which a new or revised DPIA is required.

vi. *Sixth*, Ms Thompson, the spokesperson for PHE, stated in plain terms that no DPIA has been conducted for the Programme. Indeed, Ms Thompson was unequivocal that one *was* being conducted. DHSC have not said that Ms Thompson was incorrect, despite us asking if she was.

We note that, by email of 23 June 2020, the DHSC claim that "the proper focus instead is on whether those DPIAs (single or multiple) identify the relevant risks presented by the Programme". However, on the basis of publicly available material, it is apparent that there is a significant change in risk: the processing operations envisaged under the testing system and CTAS is different in nature and scope to the processing undertaken pursuant to the Programme. Accordingly, it follows that the existing DPIA(s) undertaken in relation to the testing system and CTAS are most unlikely to have properly identified and assessed all of those new and different risks inherent in the Programme.

Furthermore, identifying whether there is a change in the risk is only possible once there has been a proper assessment of the nature of data collected, purposes of the processing, recipients of the data, risk (including risk sources, potential impacts, threats etc.) and security measures in place. Similarly, an assessment of proportionality and necessity is also only possible once those factors have been considered.

We also note that the DHSC stated that it had "set out the DPIAs that had been undertaken" and that they "continue to be reviewed". We have not been provided with the DPIA(s) that have been undertaken nor what processing operations they cover, despite asking for the same. However, if, as the DHSC say, the DPIA(s) only relate to the CTAS system and parts of the testing system, the basis for the claim that there is no change in risk in respect of the processing operations undertaken pursuant to the Programme compared to those systems is not apparent.

[6] Per WP Guidelines on the need for a reviewed DPIA.

For the reasons set out above, any DPIA(s) for the CTAS system and parts of the testing system would be insufficient to cover the "processing operations" being undertaken in the Programme. In these circumstances, a new or revised DPIA, which addresses the risks of the processing of personal data under the Programme, is plainly required to satisfy the requirements of Article 35 of the GDPR.

6. Remedies

In light of the above, our clients request that you:

i. accept that the DPIA conducted for the CTAS system and parts of the testing system does not discharge DHSC's obligations as a data controller Article 35 of the GDPR;
ii. conduct a DPIA for the Programme which satisfies the requirements of Article 35 of the GDPR;
iii. agree to put in place any measures necessary to address the risks identified by the DPIA; and
iv. agree to pay our clients' legal fees, given the concessions that have already been made following their correspondence and the nature of the conduct of the DHSC in responding to their correspondence. The DHSC should note that those fees come from not-for-profit funds and therefore could be reallocated to our client's wider aims.

Please note that our clients' only interest is for the Programme to operate with due regard to data protection and the rights of data subjects. Such considerations should be integral to the proper deployment of the Programme, particularly in light of criticism that the Programme has been rushed out and is not "fit for purpose".

7. Disclosure

We ask that you address the following requests. When replying please bear in mind the third bullet point at page 4 of the *Treasury Solicitor's 2010 Guidance on Discharging the Duty of Candour and Disclosure in Judicial Review Proceedings, R (Bilal Mahmood) v SSHD* [2014] UKUT 439 at §23 and *Citizens UK v SSHD* [2018] 4 WLR 123, §§105-106(1)-(5). If you are unable or unwilling to address any particular request, please state why, giving full reasons.

Please provide:

i. a copy of the DPIA(s) conducted to date in respect of the CTAS system and the testing system;

ii. a copy of all notes, memos and other records relating to the decision to conduct a DPIA for the CTAS system and testing system;

iii. a copy of all notes, memos and other records relating to the decision that the DPIA(s) conducted for the CTAS system and testing system was sufficient to satisfy the obligations on DHSC in respect of the processing undertaken under the Programme;

iv. a copy of all notes, memos and other records relating to the decision to not conduct a separate DPIA in relation to the processing undertaken pursuant the Programme;

v. a copy of any correspondence with the Information Commissioner's Office relating to the decision to conduct, or not conduct, a DPIA in respect of the processing envisaged under the CTAS system and/or the testing system and/or the Programme;

vi. a copy of any relevant correspondence with PHE and/or NHSX;

vii. documents relating to the security and data protection arrangements in place with third parties accessing the Programme.

This list is for illustrative purposes only. Please also provide any other disclosure as may be relevant to the determination of our clients' claim.

8. Response

Our client's request a response within 7 days of this letter, by 8 July 2020. A truncated timeframe is justified considering (1) the prior correspondence between the parties and (2) that the Programme is fully operational.

We look forward to hearing from you.

Yours sincerely

AWO

cc. (1) Duncan Delbie, PHE
(2) Matthew Gould, NHSX