ORG OPEN RIGHTS GROUP

DATA PRIVACY AND THE INFORMATION COMMISSIONER'S OFFICE DURING A CRISIS: LESSONS LEARNED FROM THE COVID-19 PANDEMIC

May, 2023

ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

Our work on data protection and privacy includes challenging the immigration exemption to UK data protection law, defending the General Data Protection Regulation (GDPR) from attempts to water down its provisions, and challenging uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

EXECUTIVE SUMMARY

Overview

Three years after the start of the pandemic, it is critical to assess how government actions and oversight by the Information Commissioner's Office (ICO) during COVID-19 circumvented data protection safeguards in the UK. This report comes at a time when the government is proposing changes to UK data protection law, which will weaken the rights of individuals and reduce the accountability of corporations. It comes when hospitals are being forced to share patients' data multinational corporations like Palantir,[1] who in turn are vying for a multi-million pound contract for the NHS Federated Data Platform. It provides a foundation to analyse these threats so that the data protection rights of people in the UK data protection can be strengthened not weakened.

Divided into four sections, the report (1) examines three case studies of data use in pandemic public health programmes, (2) compares the ICO's response to that of other European data protection authorities and UK regulators, (3) analyses the future impact of new changes to data protection law and (4) sets forth policy recommendations for the government and ICO.

Public health case studies

The Covid-19 pandemic prompted the use of new and wide-reaching technology as part of a public health response, saw the unprecedented generation, storage, and analysis of public health data, and revealed cracks in the UK's data protection regime. An analysis of the NHS Test and Trace, NHS Contract Tracing App and NHS Datastore revealed holes in the programmes' transparency and accountability, excessive retention of data, missing and late Data Protection Impact Assessments (DPIAs), and the involvement of private companies without proper safeguards. Additional concerns were raised that the large datasets created, originally justified by an emergency, would be used in ways that were not originally intended, also known as 'mission creep'.

For each programme, the public face of the ICO was largely hidden, suggesting it was unwilling to take strong enforcement action, or appeared late in the game. In the case of Test and Trace, the ICO was pushed to action by public pressure, and eventually conducted a consensual, remote audit of the programme but did not follow up on the many data protection concerns raised by its findings. For the NHS Contract Tracing App, the ICO engaged but failed to prevent clear data protection issues with the centralised version of the app, the choice of which caused significant delays. Additionally, the regulator was noticeably absent from discussions regarding the NHS Data Store, and continues to have a limited, hands-off approach to the Federated Data Platform. Government meanwhile claimed credit for consulting with the ICO in private on many of these matters.

1 https://www.opendemocracy.net/en/palantir-peter-thiel-nhs-england-foundry-faster-data-flows/

The ICO in Context

In comparison to other European data protection authorities and UK regulatory bodies, the ICO did not perform sufficiently well during the pandemic. The regulator was reluctant to take enforcement action and failed to create updated response protocols for future emergency situations, prioritising easing requirements for businesses over consumer protection. The ICO faded into the background of data protection conversations when it should have been a key player, leaving civil society and the public to ask challenging questions and demand critical data protections. By taking a behind the scenes approach, its impacts were unclear, and its independence could be called into question.

The Data Protection and Digital Information Bill

The government's planned changes to data protection law through the Data Protection and Digital Information (DPDI) Bill will exacerbate the concerns raised by the three Covid-19 public health case studies. The Bill will weaken data protection rights, water down accountability requirements, further reduce the independence of the ICO, and empower the Secretary of State with undemocratic controls over data protection.

Policy recommendations

To improve the strength of data protection standards and future responses to emergency situations, the ICO must move away from its 'critical friend' approach and use of non-binding reprimands and take stronger enforcement action against both companies and the government when they breach data protection law. The ICO must also implement protocols for emergency situations that will allow the regulator to respond quickly and provide thorough oversight during a crisis.

In addition, the government must drop the DPDI Bill. The Bill presents a clear threat to the UK's data protection framework and would further exacerbate the many issues identified with data protection for public health data during the pandemic. Overall, the UK needs more robust data governance and accountability requirements, a more objective and independent ICO, and stronger GDPR complaint mechanisms. We set forth a series of additional recommendations that would help achieve this aim, including:

- Establishing a duty for public and private organisations to publish accountability documents such as DPIAs.
- Ensuring government departments have a thorough understanding of when and how to use DPIAs, starting with an ICO-led audit of key government departments' use of DPIAs and the quality of their Data Protection Officers (DPOs).
- Moving responsibility for appointing the Information Commissioner from the government to Parliament.
- Implementing Article 80(2) of the UK GDPR to allow public interest organisations to bring opt-out representative actions.
- Involving the public more thoroughly in the ICO's work by running regular public consultations or deliberative exercises.

FOREWORD BY MARTIN BLANCHARD KEEP OUR NHS PUBLIC DATA WORKING GROUP

In this in-depth report, ORG presents a compelling account of the neglect of regulatory protection for our personal health data during the early part of the COVID pandemic: our data was handed over to a consortium of US corporations to develop a COVID data store, while numerous other companies were contracted to provide a 'Test and Trace' service and the NHS COVID app. This all happened with little public discussion, consultation, or debate, and without our consent. It was done even though government knew from early on that people were very unlikely to want to share their personal data with private companies due to a lack of trust, especially if data were to be used for commercial purposes.[2],[3]

Although other European countries took action to protect data, in the UK, the Information Commissioner's Office (ICO) and government failed to make sure that our personal data was safe from potential exploitation: the necessary legal protections went missing. This has had implications for the trust the public has in the government, with significant repercussions for our health.

Trust in technology such as information systems is often based on trust in the people and organisations that control them, rather than the system itself. This is confirmed by a large-scale survey examining attitudes towards the 'NHS' COVID app (n = 1,001). It showed a 'lack of trust' in the UK government, and even lower levels of trust in private contractors, before the app was released, and this persisted after release hindering app adoption and effectiveness.[4] Levels of uptake were around 50%, low enough to cause great concern, given the World Health Organization's (WHO) recommendation[5] and the Scientific Advisory Group for Emergencies'(SAGE) agreement of the need to trace 80% of contacts within three days to contain the infection.[6]

To increase public trust and improve intervention effect, the WHO has stressed the importance of appropriate oversight for the governance of Digital Contact Tracing apps.[7] Similarly, detailed evidence from the People's Covid Inquiry (PCI) indicates that public confidence was lost when there were serious questions of data confidentiality and effectiveness with the privately contracted app to aid contact tracing. Meanwhile other countries were developing more

2 Ghafur S, Van Dael J, Leis M, Darzi A, Sheikh A. Public perceptions on data sharing: key insights from the UK and the USA. The Lancet Digital Health. Published Online July 24, 2020 https://doi.org/10.1016/S2589-7500(20)30161-8

3 https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2018/09/how-the-uk-can-win-the-artificial-intelligence-ai-race.pdf

4 Dowthwaite L, Wagner HG, Babbage CM, Fischer JE, Barnard P, Nichele E, et al (2022) The relationship between trust and attitudes towards the COVID-19 digital contact-tracing app in the UK. PLoS ONE 17(10): e0276661. https://doi.org/10.1371/journal.pone.0276661

5 https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf?sequence=24&isAllowed=y

6 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940942/S0402_Thirty_second_SAGE_meeting_on_COVID-19.pdf

7 https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

effective apps, with greater data protection accompanied by greater public confidence[8]. Other evidence from the inquiry highlights the growing public (and considerable General Practitioner) opposition to the use of their data without transparency and consent, with one million people choosing to opt out of a government plan to transfer over 50 million GP-held patient records to NHS Digital in July 2021. The data processor was apparently to be Palantir, a private US corporation with a well-documented and highly controversial history.

Further international analyses have confirmed the role of trust as a major factor in outcomes during COVID. A comparison of 177 countries9 has shown that variation in rates of COVID infection and fatality could not be explained by political factors (such as democracy and populism); the effectiveness of the state; healthcare (such as the number of hospital beds or universal health coverage); or social factors (such as economic inequality or trust in science). However, countries with measures of high levels of trust in government had statistically significant lower infection rates, and among middle-income and high-income countries, these measures of high levels of trust were also associated with higher COVID-19 vaccine coverage. It was calculated that if these associations were to be causal, an increase in trust that matched the level in Denmark, which was in the 75th percentile across these spectrums, might have reduced global infections by 12·9% (5·7–17·8).

Trust is an area where governments could and should act for the sake of people's lives. In Public Health crises, personal data is an important resource but to take it without people's knowledge, to neglect to protect it, or to allow its commercial use without consent will increase our distrust and lower our willingness to take up government or private company interventions involving its use. The design of services requiring technology and its wide uptake, such as in public health, should embed consideration of the complexities of trust and the context in which the technology will be used. This must include ways in which to ensure the enforcement of our current governance and protections. It also means that the planned weakening of the independence of the ICO, the removal of Data Protection Impact Assessments and the multiple other changes in version 2 of the Data Protection and Digital Information Bill now in Parliament which wouldmake it easier for commercial use of our data without consent, must be halted.

---

8 https://36085122-5b58-481e-afa4-a0eb0aaf80ca.usrfiles.com/ugd/360851_310fe297a8ec410dba2f5888d6ff3d19.pdf Page 169 7.5.9

9 Pandemic preparedness and COVID-19: an exploratory analysis of infection and fatality rates, and contextual factors associated with preparedness in 177 countries, from Jan 1, 2020, to Sept 30, 2021
COVID-19 National Preparedness Collaborators* Lancet 2022; 399: 1489–512 Published Online February 1, 2022
https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(22)00172-6/fulltext

1 INTRODUCTION

In spring 2020, the spread of COVID-19 across the globe upended daily life as people became sick, hospitals became overwhelmed and unprecedented lockdown restrictions were put in place. In response, people in the UK demonstrated enormous courage and resolve. The overwhelming majority of the public followed lockdown guidance, key workers continued to keep public services and supermarkets running, and many people volunteered their time to support critical services. Many people also shared their personal data with public health officials to aid COVID-19 tracking and health research.

However, the government took advantage of this public goodwill by ignoring fundamental privacy and data protection measures in their pandemic response. When creating public health mechanisms like the NHS Test and Trace system, the NHS Contract Tracing app, and NHS Data Store, the government failed to properly conduct Data Protection Impact Assessments (DPIAs), retained data excessively, undermined data subjects' rights, and entered into data sharing agreements with private companies like Palantir. Doing so allowed private corporations to take advantage of the situation to siphon sensitive data from national public health databases.

While issues like pandemic price gouging were blatantly obvious, the exploitation of people's personal data is arguably more insidious because the practice is less visible and more difficult for people to track. However, the real life consequences are just as serious. When companies are given access to vast amounts of public data with little oversight they will invariably use our data without proper consent for commercial purposes. Corporations get rich using data to profile, manipulate, and discriminate, almost always at the expense of society's most vulnerable groups.

It is perhaps even more serious that the government was playing fast and loose with public trust when it needed it most. National health programmes like the contact tracing app and Test and Trace can only succeed with significant public participation. However, Matt Hancock, then Secretary of State for Health, showed clear disregard for legal requirements and due diligence, boasting that his government would "not be held back by bureaucracy" when questioned about the government's failure to follow data protection law in the rollout of Test and Trace.[10] By ignoring the importance of proper data protection in the design and implementation of these programmes, the government risked backlash and refusal to participate, which could have greatly exacerbated the spread of Covid-19. Privacy and data governance should support, rather than undermine, the government during national crises like the pandemic.

Throughout the pandemic, Open Rights Group (ORG) raised the alarm about the lack of regard toward privacy and data protection. In particular, ORG was concerned about the lack of urgency from the Information Commissioner's Office (ICO), the UK's independent regulatory body for data protection. At a time when the ICO's oversight was critical, the regulator pared back its duties and adopted a less stringent 'critical friend' approach towards government actions. An open letter coordinated by ORG arguing that the ICO was failing to protect the privacy and data of UK citizens was signed by over twenty cross-party Members of Parliament (MPs).[11]

Three years on from this crisis for public data, it has become clear that both the government and the ICO have learned little from the experience. There has been no official review of data protection policy during the pandemic, nor has it been a focus of Parliamentary attention. Data protection concessions won by civil society groups during the pandemic have for

10 https://twitter.com/OpenRightsGroup/status/1285260608875700225

11 https://www.wired.co.uk/article/ico-data-protection-gdpr-enforcement

the most part, been ignored. The government's relationship with Palantir, which began with an infamous £1 contract for the NHS data store, is ongoing, with the company favoured to win a £360 million contract for the NHS Federated Data Platform.[12] An openDemocracy report has revealed that in February 2023, NHS hospitals were ordered to upload patient data to a new central database that uses Palantir's Foundry software.[13] Despite all of this, the ICO continues to favour a consultative approach over an adversarial one and has been reluctant to take enforcement action on government programmes, even after clear violations of data protection law.

These issues will only worsen with the government's proposed Data Protection and Digital Information (DPDI) Bill. The proposed reforms to the UK's data protection framework will water down data subjects rights, weaken the independence of the regulator, and threaten EU adequacy. The UK is currently facing a perfect storm: non-compliant private and government actors, a reluctant regulator, and weakening regulation.

Amid this perfect storm, it is critical to take a step back and assess how government and businesses responses to COVID-19 challenged data protection in the UK. This report, which focuses on the ICO's oversight and enforcement in key public health data case studies provides a foundation to analyse the regulator's current weaknesses and provide recommendations to strengthen UK data protection moving forward.

This report is based on desk research and interviews. The desk research was conducted through a review of public materials, including legal documents, DPIAs, news articles, civil society and government press releases, and responses to Freedom of Information (FOI) requests. In addition, we conducted interviews with two data protection lawyers for background information on European data protection authorities and the ICO's history with regard to enforcement action. The report is organised into six sections:

1. **Introduction.** Section One lays out the foundations of the report, emphasizing the importance of analysing how government and businesses responses to COVID-19 challenged data protection in the UK, particularly in light of the continued development of public health programmes and new data protection legislation.

2. **UK Covid-19 Programmes.** This section sets out key data protection issues and the ICO's response across three case studies: the NHS Test and Trace, the Contact Tracing App, and the NHS Datastore.

3. **The ICO in Context.** This section analyses the ICO's regulatory approach by drawing on examples from Norway and France's data protection agencies, the UK's Competition and Markets Authority and the UK's Financial Conduct Authority.

4. **The Data Protection and Digital Information Bill.** This section looks at the government's data protection bill which is currently making its way through Parliament, breaking down key issues with the Bill that would exacerbate data protection issues in future emergency situations.

5. **Policy Recommendations.** This section provides recommendations for improving future responses to emergency situations, ensuring the ICO's role in upholding strong data protection standards, and creating a comprehensive data protection framework.

6. **Conclusion.** Section Six concludes the report, summarising key findings and arguments while making a case for a better way forward.

12 https://www.digitalhealth.net/2022/12/federated-data-platform-palantir-juggernaut-continues/; https://www.digitalhealth.net/2023/01/palantir-gets-11-5m-six-month-nhs-contract-extension/

13 https://www.opendemocracy.net/en/palantir-peter-thiel-nhs-england-foundry-faster-data-flows/

2 CASE STUDIES: NHS TEST AND TRACE, THE NHS CONTACT TRACING APP, THE NHS DATASTORE

In this section, we analyse the ICO's approach to the UK Government's failure to implement proper data protection requirements in three Covid-19 programmes: NHS Test and Trace, the Contact Tracing App, and the NHS Datastore.

Each of these initiatives played an arguably pivotal role in shaping the UK's nationwide response to Covid-19. Test and Trace and the Covid-19 App formed the backbone of UK contact tracing efforts, while the NHS Datastore was used to inform policymaking and public responses to the crisis, such as decisions to introduce or remove lockdown restrictions.

These programmes also share significant similarities in how the law of data protection applied to them. They are characterised by:

- Very large scale and often novel processing of special category personal data by public authorities and processors on their behalf.
- The involvement of numerous third parties in the processing of sensitive public data. The programmes – partly because of their size – involved public authorities engaging complex networks of processors, notably including companies headquartered in the United States: Test and Trace involved Amazon Web Services, Serco UK, and the SITEL Group;[14] the Contact Tracing App also used Amazon Web Services, implying data transfers to the US; and the Datastore was implemented by companies such as Microsoft and Palantir.
- Concerns about further use of the collected data. Given the exigencies of the pandemic, opposition to the primary purposes of the three programmes was limited (though by no means non-existent). Developments since have led to concerns that large datasets, originally justified by an emergency, will be made use of in new and unexpected ways. This was a concern of the ICO in relation to the Contact Tracing App[15] and is most notable in relation to the Datastore.[16]

In turn, the data protection compliance and regulatory issues that arose from these programmes revealed two main deficiencies.

14 The Programme involves the sharing of data with Amazon Web Services, Serco UK and the SITEL Group. The ICO found that this led to lack of clarity about data flows: "Test and Trace needs to carry out a comprehensive data mapping exercise to ensure that data flows are identified and reflected in relevant information asset registers (IARs) and within the record of processing activities (RoPA). Processes needed to be put in place to ensure that the RoPA and IARs are regularly reviewed and kept up to date." https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019279/executive-summary-of-the-nhs-test-and-trace-audit-report.pdf

15 E.g. ICO found "it will be possible for those developing COVID-19 contact tracing apps – anticipated to be whitelisted PHAs and similar organisations – to design apps that use the CTF but also collect other data and use other techniques beyond those envisaged by the CTF." https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

16 See e.g. comments from the National Data Guardian: https://www.gov.uk/government/news/in-pursuit-of-balance-unlocking-the-power-of-data-whilst-preserving-public-trust

2.1 PUBLIC HEALTH PROGRAMMES WERE DEPLOYED UNLAWFULLY, AND UNDERPINNED BY NEGLIGENT DATA GOVERNANCE

All three programmes failed to comply in full with the requirement in Article 35 GDPR for DPIAs. This was most notable for Test and Trace[17] and for the Datastore, where no DPIA was entered into with providers prior to entering in agreements with them.[18] The three programmes often fell short of compliance with data protection legislation and gave rise to concerns about interference with privacy rights on a national scale.

These shortcomings gave rise to well-documented harms and data misuses, including:

- Confidential contact tracing data being leaked on social media channels by Test and Trace personnel,[19] being abused to harass women,[20] or being lost due to its storage on an excel sheet[21]. By carrying out a DPIA, these risks could have been identified and mitigated.
- The NHS Covid-19 app roll out being delayed in order to switch to a decentralised model of contact tracing.[22] Independent experts[23] as well as the Joint Committee for Human Rights[24] had warned that it was hard to prove the efficacy and justify the necessity of a centralised digital contact tracing system. Had the Government taken privacy implications into due consideration, they would have developed a decentralised app from the outset without the need to perform a U-turn.
- Multinational corporations being given access to sensitive public health data. Palantir's continued and growing involvement in the UK health service and wider public services[25] has been of particular interest and concern, given the scale and complexity of its operations, its well-documented use of data for law and immigration enforcement purposes, and the lack of effective rights and enforceable remedies against misuse of data for national security purposes in the United States. Several civil society organisations, including Foxglove, have spoken out against the involvement of Palantir in the NHS datastore, arguing that it will give predatory private researchers and pharmaceutical companies access to sensitive public health data for profit.[26]

17 See e.g. for Test and Trace https://www.openrightsgroup.org/press-releases/government-admits-test-and-trace-unlawful/

18 For Test and Trace, the ICO found "There was also no monitoring of compliance with data protection policies and procedures within the Test and Trace programme" (emphasis added): https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019279/executive-summary-of-the-nhs-test-and-trace-audit-report.pdf

19 The Times "Coronavirus contact tracers sharing patients' data on WhatsApp and Facebook." Source: https://www.thetimes.co.uk/edition/news/coronavirus-contact-tracers-sharing-patients-data-on-whatsapp-and-facebook-rg3zqn5l6

20 The Telegraph "Test and trace is being used to harass women – already." Source: https://www.telegraph.co.uk/women/life/test-trace-used-harass-women-already/

21 https://www.bbc.co.uk/news/technology-54423988

22 Source: https://www.bbc.com/news/technology-53095336

23 Matthew Ryder QC, Edward Craven, Gayatri Sarathy & Ravi Naik (AWO), COVID-19 & Tech responses: Legal opinion. Retrieved at: https://www.awo.agency/covid-19-legal-opinion.pdf

24 Joint Committee on Human Rights, Human Rights and the Government's Response to Covid-19: Digital Contact Tracing. Retrieved at: https://committees.parliament.uk/publications/992/documents/7782/default/

25 See e.g. past involvement in processing large amounts of data on adult social care: https://atamis-1928.cloudforce.com/sfc/p/#0O000000rwim/a/4J000000NLZI/BbXY3NqCj1neqPYbc6W2A3kTWC9FYCFcuqSDC5sBTI4 and plans to extend the work on the Datastore into an NHS Federated Data Platform: https://www.find-tender.service.gov.uk/Notice/008755-2022

26 https://www.foxglove.org.uk/2022/09/30/doctors-not-dashboards-360m-palantir/

2.2 THE ICO ACTED AS A "CRITICAL FRIEND" AND DID NOT ENFORCE THE LAW EFFECTIVELY

The case studies show that the ICO was reticent to take strong action against data protection infringements, which eventually led to these programmes falling short of important safeguards and data protection requirements.

Further, the Commissioner gave more importance to engaging with the Government as a "critical friend", rather than holding government departments to account and promoting diligence and compliance with the law. In particular:

- The ICO's approach of engaging constructively did not prevent Test and Trace from being deployed unlawfully, exposing the public to significant risks and harms. After a consensual audit carried out by the ICO in January 2021, the Department for Health and Social Care (DHSC) still falls short of foundational elements of data governance, such as record-keeping.[27]
- The ICO acted as a "critical friend" after the Government decided to reject the Commissioner's opinion, which favoured a decentralised model of digital contact tracing, and pursue a more invasive, centralised approach. In an avoidable u-turn, the Government eventually switched to a decentralised model instead, adding considerable delays to the roll out of the App
- The NHS Datastore falls short of several critical data protection requirements and is poised to transfer NHS patients' data at scale to Palantir, a counter-terrorism data analytics company based in the United States. The ICO admittedly had limited discussions with NHS Digital and NHS England regarding the platform, but evidence suggests that little to none of the shortcomings identified in this report have been addressed to this date.

The ICO have a statutory duty to prioritise monitoring and enforcement of data protection law. While the law provides a certain degree of discretion, each of these cases studies suggests that the ICO may lack sufficient independence from the Government to perform their regulatory function with all due diligence. The case studies below provide more detailed explanations of these issues, delving further into the actions of the government and the ICO's response to each programme.

CASE STUDY A: NHS TEST AND TRACE

In May 2020, the DHSC began the Test and Trace programme for the UK. This comprised both manual contact tracing and digital contact tracing via a smartphone app (see Case study B: NHS Contact Tracing App). The aim was to identify individuals infected with Covid-19 and trace their contacts to limit further transmission . It involved around 600 testing sites and several laboratories across the country,[28] operated by 3,000 health professionals and 18,000 call handlers.[29]

27 https://ico.org.uk/action-weve-taken/enforcement/department-of-health-and-social-care/

28 https://www.nao.org.uk/wp-content/uploads/2020/12/The-governments-approach-to-test-and-trace-in-England-interim-report.pdf (p.9)

29 https://committees.parliament.uk/work/906/covid19-test-track-and-trace-part-1/publications/

TEST AND TRACE TIMELINE

25 May 2020 — DHSC announces the launching of the NHS Test and Trace programme.[30]

28 May 2020 — The NHS Test and Trace officially launches. A privacy notice for the programme is published.[31]

2 June 2020 — ORG instructs legal firm AWO to act on their behalf on this matter, and send a letter to DHSC inquiring about the Test and Trace programme, including the 20-year data retention period and the DPIA. In response, DHSC does not offer a rationale for the 20-year retention period but amends the retention period to eight years. On the DPIA, DHSC gives no response.

5 and 8 June 2020 — AWO sends follow up emails to DHSC regarding questions on the DPIA for the Test and Trace programme.

10 June 2020 — DHSC states that it is "committed to" reply by 16 June.

16 June 2020 — DHSC states that it "will reply" by 22 June 2020. AWO asks if the Test and Trace and programme was deployed without a DPIA having been conducted. On this, DHSC states that DPIAs were "undertaken for both the testing and contract tracing advisory service (CTAS) aspects of the programme."

18 June 2020 — AWO seeks clarification of the CTAS system and how it relates to the Test and Trace programme.

19 June 2020 — DHSC replies, but does not clarify if a DPIA had been conducted for the Test and Trace programme as a whole.

23 June 2020 — DHSC confirms that no DPIA was conducted for the Test and Trace programme as a whole, and has only been conducted for CTAS.

25 June 2020 — AWO seeks clarity on whether the CTAS system is the same system as the Test and Trace programme.

26 June 2020 — DHSC confirms that CTAS is the website for the Test and Trace programme.

1 July 2020 — AWO sends a pre-action letter to DHSC.[32]

15 July 2020 — The Government Legal Department responds to the pre-action letter, in which the DHSC admit that it had not conducted a DPIA for the Test and Trace programme as a whole.[33]

20 July 2020 — Caroline Lucas MP tables a parliamentary question during the Government coronavirus statement, asking why the Secretary of State for Health considered DPIAs "optionals". Matt Hancock, then Secretary of State for Health, answers "Mr. Speaker, I will not held back by bureaucracy.".[34]

30 https://www.gov.uk/government/news/government-launches-nhs-test-and-trace-service

31 https://web.archive.org/web/20200604135952/https://contact-tracing.phe.gov.uk/help/privacy-notice

32 https://www.awo.agency/2020-07-01-Pre-Action-Letter.pdf/

33 https://www.awo.agency/2020-07-15-PAP-Response-Letter.pdf

34 https://twitter.com/OpenRightsGroup/status/1285260608875700225

DATA PROTECTION ISSUES WITH THE TEST & TRACE PROGRAMME

Lack of DPIA

A DPIA should have been carried out for the NHS Test and Trace programme in its entirety, prior to the commencement of the programme. In their response to AWO's pre-action letter, the Government admitted that such a DPIA had not been conducted.[35]

Article 35(1) of the General Data Protection Regulation (GDPR) states that, before data processing begins, a data controller is required to carry out a DPIA where that 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". Article 35(3) specifies that DPIAs are, in particular, required for "processing on a large scale of special categories of data", which includes health data. These obligations apply to public authorities and should therefore consider the impact on data subject rights under the GDPR and include an assessment of any potential infringements with the European Convention on Human Rights (ECHR), particularly the right to privacy under Article 8.[36]

Excessive data retention

The NHS Test and Trace programme's original retention period of 20 years appeared excessive and led to concerns that the data would be retained for purposes other than Test and Trace. In correspondence with AWO, DHSC did not give a rationale for this retention period but amended the period to eight years (no rationale was provided for the new retention period, either). DHSC's failure to provide any reasoning behind its data retention period and its immediate reduction to a shorter period under questioning demonstrates the organisation's lack of transparency and clarity. It is likely that DHSC either chose arbitrary lengths of time or was intending to reuse the data for other purposes.

Under Article 5(1)(e) of the GDPR, personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed", which is known as the 'storage limitation' principle. Recital (39) clarifies that the period for which the personal data are stored is limited to a strict minimum and time limits should be established for erasures or for periodic review to ensure that the retention of the data is necessary. Article 5(1) further specifies that "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject". As such, while health research and scientific purposes are legitimate bases for longer storage periods under GDPR, they must be an explicit purpose of the programme, and subject to appropriate oversight measures. Section 19 of the Data

35 https://www.awo.agency/2020-07-15-PAP-Response-Letter.pdf (p.4)

36 R (Bridges) v Chief Constable of South Wales Police [2020] 1 WLR 672, para. 151, available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

Protection Act 2018 also sets out specific provisions that must be followed for this type of processing including, for example, that the processing must be necessary for the purposes of "approved medical research".[37]

To determine how long data should be retained, three other principles under the GDPR are also relevant. This includes: (i) the 'purpose limitation' principle, which requires that the data processed is connected to specified, explicit and legitimate purposes and only other compatible further purposes,[38] (ii) the 'data minimisation' principle, which requires that the data collected for the processing purpose is limited to what is necessary for that purpose,[39] and (iii) the principle of lawfulness, fairness and transparency, which requires that the processing has a legal basis and meets the applicable legal requirements, considers the interests of the data subject and is made known to the data subject in an accessible manner.[40]

The ICO's response to the Test and Trace programme

In response to AWO's pre-action letter, the government confirmed that the ICO was constructively engaged in the completion of a DPIA for the Test and Trace programme "and also in relation to elements of the substantive processing".[41] However, the regulator was still criticised for "failing to hold the government to account for its failures in the NHS [Test and Trace] programme."[42] It was accused by MPs of "sitting on its hands" and not using its powers to ensure that the government complied with data protection law.[43]

In January 2021 – six months after the government admitted that a DPIA had not been conducted – the ICO began a consensual audit of the Test and Trace programme, assessing the processing of personal data for the Test and Trace programme.[44] The audit was provided to DHSC in July 2021, and the Executive Summary was published in December 2021 (the full audit has never been made public).[45] The purpose of the audit was to provide an opinion on the extent to which DHSC was "complying with data protection legislation and highlight any areas of risk to their compliance".[46] The audit revealed "a number of key requirements that were not yet in place,[47] and made 77 recommendations.

37 https://www.legislation.gov.uk/ukpga/2018/12/section/19

38 Article 5(1)(b), available at: https://gdpr-info.eu/art-5-gdpr/.

39 Article 5(1)(c), available at: https://gdpr-info.eu/art-5-gdpr/.

40 Article 5(1)(a), available at: https://gdpr-info.eu/art-5-gdpr/.

41 https://www.awo.agency/2020-07-15-PAP-Response-Letter.pdf (p.4)

42 https://www.theguardian.com/uk-news/2020/aug/21/mps-criticise-privacy-watchdog-information-commissioner-nhs-test-and-trace-data; https://www.openrightsgroup.org/press-releases/cross-party-group-of-mps-challenge-information-commissioner-over-data-protection-failure/

43 Ibid.

44 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019279/executive-summary-of-the-nhs-test-and-trace-audit-report.pdf

45 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019279/executive-summary-of-the-nhs-test-and-trace-audit-report.pdf (p.4)

46 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019279/executive-summary-of-the-nhs-test-and-trace-audit-report.pdf (p.3)

47 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019279/executive-summary-of-the-nhs-test-and-trace-audit-report.pdf (p.5)

The urgent and high-priority recommendations included: ensuring appropriate oversight and assurance for information governance; conducting a comprehensive data mapping to reflect data flows in relevant information asset registers; and developing a policy on sourcing, awarding and managing contracts involving the processing of personal data by data processors and third parties. The audit noted: "Data protection considerations need to be built into the contract approval and management processes including, where relevant, the completion of DPIAs. Where current arrangements have not been subject to some form of privacy risk assessment these should be undertaken retrospectively and action taken where required."[48]

The wording indicates that the audit may have revealed additional third-party contracts through Test and Trace where a DPIA or risk assessment was not conducted. These findings are especially concerning as extensive public data could have been shared to third-parties with little to no oversight of their use of the data.

CASE STUDY B: NHS CONTACT TRACING APP

The UK government originally planned to release a centralised contact tracing app developed in-house with Pivotal, who were given a £2 million contract for the work. Eventually, after a failed trial of the app on the Isle of Wight, the government opted for the Google/Apple Exposure Notification (GAEN) system to build a decentralised contact tracing app, which was launched in September 2020.[49] The NHS contact tracing app complemented the traditional contact tracing under the government's Test and Trace programme.[50] The app included functionality that allowed users to check into events and venues with a QR code.

Centralised and decentralised contact tracing apps process and store user data differently. With centralised models, a central server generates user identifiers. When a user records a positive Covid-19 diagnosis on their app, it sends the central server a list of identifiers for other users who were physically proximate to the Covid-positive user within a window of time. The central server calculates the level of risk for each exposed user and sends notifications to those who meet the risk threshold. With decentralised models, identifier generation takes place locally on device (and not on a central server). Consequently, decentralised models provide stronger levels of data protection to users.

48 Ibid, p.8

49 https://www.thebureauinvestigates.com/stories/2020-06-13/where-is-matt-hancocks-contact-tracing-app

50 https://www.gov.uk/government/news/nhs-covid-19-app-launches-across-england-and-wales

CONTACT TRACING APP TIMELINE

March 2020: NHSX (the former technology arm of the NHS) partnered with VMware Pivotal Labs to develop a contact tracing app[51] in a contract worth almost £2 million.[52] At the time that the NSHX app was under development, the government decided against using the GAEN API due to its limitations, such as the inability to detect user proximity whilst the app was running in the background.[53]

April 2020: NHSX published a blog post announcing the development of the centralised NHS contact tracing app. It stated that the data processed would "only ever be used for NHS care, management, evaluation and research" and that the NHS will always comply with the law around the use of personal data.[54] The app was also endorsed by the National Cyber Security Centre, which stated that while the app used a centralised model for contact tracing, the NHS had implemented measures "to properly protect privacy and security."[55] The DPIA for the app was not published until 6 May 2020.[56]

4 May 2020: A trial for the centralised NHS app was announced; it would launch on the Isle of Wight on 8 May. On the same day, the Information Commissioner provided evidence to the Joint Human Rights Committee of the UK Parliament, where she discussed the ICO's involvement with the app. She disclosed that the ICO had yet to receive a DPIA for the app, but expected one imminently.

6 May 2020: The DPIA for the contact tracing app was published.[57]

8 May 2020: The contact tracing app trial began on the Isle of Wight. Around 40% of the population downloaded the app during the trial. [58] [59]

9 May 2020: Dr. Michael Veale released his analysis of the DPIA, which identified severe data protection concerns.

Mid-May: The centralised app was not released to the whole country as originally planned.[60]

18 June: The government announced the next phase of app development and its shift to a decentralised Google/Apple solution. The official statement focused on technical challenges and field-testing raised by the trial and did not reference any data protection concerns.[61]

Late June: The development of the app was taken over by Zuhlke,[62] a global innovation service provider based in Switzerland, under a £4 million contract awarded by the government.[63]

13 August 2020: New DPIA for the contact tracing app is published.[64]

24 September 2020: The new NHS contact tracing app is launched.[65]

---

51 https://tanzu.vmware.com/content/blog/developing-during-a-pandemic-the-lessons-we-learned

52 https://www.thebureauinvestigates.com/stories/2020-06-13/where-is-matt-hancocks-contact-tracing-app

53 https://tanzu.vmware.com/content/blog/developing-during-a-pandemic-the-lessons-we-learned

54 https://healthtech.blog.gov.uk/2020/04/24/digital-contact-tracing-protecting-the-nhs-and-saving-lives/

55 https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

56 https://www.dmu.ac.uk/about-dmu/news/2021/january/the-long-read-data-privacy-and-the-covid-19-app.aspx

57 https://web.archive.org/web/20200513081530/https://faq.covid19.nhs.uk/DPIA%20COVID-19%20App%20PILOT%20LIVE%20RELEASE%20Isle%20of%20Wight%20Version%201.0.pdf

58 https://transform.england.nhs.uk/news/coronavirus-test-track-and-trace-plan-launched-isle-wight/

59 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/976886/IoW_EA_report_April_2020.pdf

60 https://www.telegraph.co.uk/technology/2020/06/10/behind-delay-uks-contact-tracing-app/

61 https://www.gov.uk/government/news/next-phase-of-nhs-coronavirus-covid-19-app-announced

62 https://tanzu.vmware.com/content/blog/developing-during-a-pandemic-the-lessons-we-learned

63 https://www.thebureauinvestigates.com/stories/2020-06-13/where-is-matt-hancocks-contact-tracing-app

64 https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information-early-adopter-trial/the-nhs-covid-19-app-data-protection-impact-assessment-early-adopter-trial-august-2020

65 https://www.gov.uk/government/news/nhs-covid-19-app-launches-across-england-and-wales

DATA PROTECTION ISSUES WITH THE NHS CONTACT TRACING APP

Centralised app

Dr. Michael Veale, an Associate Professor in Digital Rights and Regulation at University College London, identified a number of concerns with first version of the contact tracing app and the original DPIA. These included:

Anonymous data

The DPIA for the original centralised NHS contact tracing app stated that it did not process "any directly identifiable information" and was designed to "preserve the anonymity of its users."[66] However, for each user, the app generated ephemeral identifiers that were shared with a central server. While this data could not directly identify individuals on its own, there are techniques that could be used to identify individuals using such data.

Under the GDPR, "personal data" is defined as "any information relating to an identified or identifiable natural person". An identifiable natural person includes a person "who can be identified, directly or indirectly, in particular by reference to an identifier", for example an identification number or location data.[67] Recital 26 clarifies that even pseudonymised data, which consists of data that can be used to identify individuals when combined with additional information, falls under the definition of personal data. It also states that to "determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used" and specifies that "account should be taken of all objective factors", including "the available technology at the time of the processing and technological developments."

Dr. Veale presented three scenarios in which re-identification could be carried out using the data collected by the app, in order to demonstrate that such data did not meet the standards for anonymity under the GDPR. [68]

Data subject rights

The DPIA incorrectly asserted that the rights of data subjects were not undermined by the app. The app potentially undermined several data subject rights under the GDPR, including the right of erasure, the right of access and the right to object.

Under Article 17 of the GDPR, data subjects have the right to have their data deleted in certain scenarios, such as where "personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed." However, the DPIA stated that while users could uninstall the app from their phone, this would not delete the data that existed in the back-end infrastructure of the app. Additionally, the app implied that users would not be able to delete their data or request the deletion of their data, and did not include an apparent legal basis to justify this restriction.

Based on the right of access under Article 15 of the GDPR, data subjects have the right to know what personal data is being processed and access a copy of that data. The design of the centralised NHS contact tracing app seemed to make such requests quite difficult, if not impossible. Veale wrote that the app could be configured differently to make it possible to act on access requests.[69]

Finally, Article 21 of the GDPR provides users with the right to object to the processing of their personal data in certain scenarios, including where the controller is processing that data for a task carried out in the public interest.[70] The DPIA for the centralised NHS contact tracing app did not address how this right would be respected, suggesting that any requests under Article 21 would be rejected; such a

66 https://mfr.osf.io/render?url=https://osf.io/download/5eb6b97c9ddd2801190971e3/?direct%26mode=render (p.3)

67 Article 4(1) GDPR

68 https://mfr.osf.io/render?url=https://osf.io/download/5eb6b97c9ddd2801190971e3/?direct%26mode=render (p.4)

69 https://mfr.osf.io/render?url=https://osf.io/download/5eb6b97c9ddd2801190971e3/?direct%26mode=render (p.8)

70 Article 6(1)(e) GDPR

restriction should require an appropriate justification set out in the DPIA.[71]

GAEN app

The decentralised version of the contact tracing app was launched with a "much stronger DPIA immediately attached".[72] The DPIA was updated in December 2020 to cover updates to the technology. However, the app still presented some data protection issues.

Automated processing

DHSC determined that Article 22 of the GDPR, which regulates processing that involves automated individual decision-making, did not apply to the app.[73] Nevertheless, DHSC stated that steps were taken to comply with this provision. However, as admitted in the DPIA for the decentralised NHS contact tracing app, the app uses an algorithm to produce a risk score for users, which may require them to follow public health advice or guidance (such as to self-isolate); as such, Article 22 may be applicable.[74]

If so applicable, Article 22(2) states that automated processing may only be carried out in three distinct instances. The second of these, under Article 22(2)(b), states that automated processing is permitted if it is "authorised by…law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interest."[75] Accordingly, in the DPIA, DHSC assert that the basis for automated processing in the contact tracing app can be found in s.2A of the NHS Act 2006; subsection (1) of that provision states that the Secretary of State "must take such steps as the Secretary of State considers appropriate for the purpose of protecting the public in England from disease or other dangers to health".[76] Subsection (2) lists what those steps could be, including "providing…facilities for the prevention, diagnosis or treatment of illness" and "providing information and advice."[77]

However, there are two potential issues with using the 2006 Act as a legal basis for automated processing under the GDPR. Firstly, the legal basis may be too broad. The DPIA states that DHSC rely on s.2A "to authorise the design, implementation and operation of the App."[78] Yet, this provision does not clearly provide a basis for the processing of personal data based on automated individual decision-making as required by Article 22(2)(b) of the GDPR. Recital (41) of the Regulation provides that, whenever a controller relies on a legislative measure to process personal data, that measure "should be clear and precise and its application should be foreseeable to persons subject to it."[79] It could be argued that s.2A of the 2006 Act does not meet this standard. Secondly, that section does not appear to meet the second part of Article 22(2)(b), which states that the measure should lay down measures to safeguard the data subject's rights, freedoms and legitimate interests. Although such measures are clearly absent from s.2A, the DPIA states that DHSC has sought to implement such measures. This includes encouraging users to phone NHS 111 if they have any questions or concerns about the notice to self-isolate as well as providing clear

71 https://mfr.osf.io/render?url=https://osf.io/download/5eb6b97c9ddd2801190971e3/?direct%26mode=render (p.9)

72 https://www.dmu.ac.uk/about-dmu/news/2021/january/the-long-read-data-privacy-and-the-covid-19-app.aspx

73 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028998/NHS_COVID_19_App_DPIA.pdf (p.50)

74 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028998/NHS_COVID_19_App_DPIA.pdf (p.50)

75 https://gdpr-info.eu/art-22-gdpr/

76 https://www.legislation.gov.uk/ukpga/2006/41/section/2A

77 https://www.legislation.gov.uk/ukpga/2006/41/section/2A

78 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028998/NHS_COVID_19_App_DPIA.pdf (p.50)

79 https://gdpr-info.eu/recitals/no-41/

explanations of how the risk score is generated by the app.[80] However, these measures do not provide an opportunity to contest the decision made as required for Article 22(2)(b).[81]

Use of Software Developer Kits

Software developer kits (SDKs) provide software tools that developers can integrate into their apps to speed up the development process and create different functionalities for the app. The GAEN API is an example of this, and the DPIA for the NHS contact tracing app explains how this is used for the contact tracing functionality.

However, the use of SDKs can introduce privacy risks for end users, especially when developers integrate proprietary SDKs offered by data-driven organisations like analytics and advertising companies.[82] For example, the use of SDKs to monitor app performance and stability may collect a user's network connectivity, Bluetooth status, battery levels and other information, and share this with the third-party that developed the SDK (sometimes without the full knowledge of the developer). In addition, some SDKs can be configured to collect more data than is needed for the particular processing purpose, such as Google Firebase.[83] A study published in July 2020 found that some Android contact tracing apps using the GAEN API collected and shared a range of extraneous data with Google servers, including the phone IMEI, serial numbers, phone numbers, WiFi MAC addresses and user email addresses.[84]

The privacy notice for the NHS contact tracing app[85] does not provide a full list of the SDKs used or whether any SDKs other than the GAEN API are used. This would be an important step in fulfilling the principle of lawfulness, fairness and transparency under Article 5(1)(a) of the GDPR,[86] especially where the data being processed by the NHS contact tracing app is sensitive in nature; Recital (60) clarifies that the specific circumstances and context should be taken into account when providing data subjects with information about how their data are being processed so as to ensure fair and transparent processing.[87] Also, as per Article 12(1), that information must provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[88]

The ICO's response to the NHS Contact Tracing app

In April 2020, the ICO released its opinion on the GAEN API, in accordance with s.115(3) of the DPA 2018.[89] The ICO stated that the API appeared to be aligned with the principles of data protection by design and by default.[90] However, it warned that those integrating the API could still configure those apps to collect data beyond that ordinarily processed by the API,[91] and emphasised that those designing contact tracing apps, "are responsible for ensuring the app complies with data protection law where it processes personal data".[92]

---

80 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1028998/NHS_COVID_19_App_DPIA.pdf (p.151)

81 A29 WP, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (3 October 2017), p.27.

82 Data Protection and Privacy: Data Protection and Artificial Intelligence, Hart Publishing, 2021, p.2.

83 Data Protection and Privacy: Data Protection and Artificial Intelligence, Hart Publishing, 2021, p.19.

84 https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

85 https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice#data-the-app-uses

86 https://gdpr-info.eu/art-5-gdpr/

87 https://gdpr-info.eu/recitals/no-60/

88 https://gdpr-info.eu/art-12-gdpr/

89 https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

90 https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf (p.8)

91 https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf (p.8)

92 https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf (p.3)

In May 2020, the ICO set out its expectations for contact tracing apps and relevant data protection requirements by publishing ten principles that developers should follow when building contact tracing apps.[93] The ICO also stated that its guidance supplemented the "ongoing conversations between the ICO and NHSX regarding its planned contact tracing app and associated activities".[94]

The ICO was involved early in the development of the centralised NHS contact tracing app. In evidence given to the Joint Human Rights Committee of the UK Parliament in May 2020, the Information Commissioner confirmed that the ICO was acting as a "critical friend" in providing NHSX with data protection advice for the app.[95] The Commissioner explained that the Data Protection Act 2018 gave the ICO the flexibility to act not just as an enforcer, but also an expert advisor, and that this was the role it played with respect to the app.[96] In doing so, she emphasised that the ICO would not "sign off" or approve any particular aspect of the app, including the decision to use a centralised model for contact tracing.[97] Instead, the Commissioner stated that it was up to NHSX to decide the purpose of the app and the mechanisms for fulfilling those purposes. If this led to a decision to use a centralised model, any data protection risks would need to be addressed and documented in a DPIA.[98] The ICO was also prepared to monitor the public response to the app, take complaints and carry out investigations and audits where needed.[99] In addition, NHSX had agreed to a voluntary audit at some point during the rollout.[100]

During the session, the Commissioner confirmed that the ICO was expecting a DPIA from NHSX for the app "very soon"[101] and that it had already received some technical material to review[102] on the same day, the contact tracing app trial on the Isle of Wight had been announced; it is therefore implied that the ICO did not expect to make any major recommendations or interventions to the app in advance of the trial, which was to begin that same week).

The DPIA for the decentralised version of the NHS contact tracing app was released in September 2020, and included regular input from the ICO. According to the regulator, while it "did not have a seat at the design table" it was consulted by the government "from the outset and provided advice on a privacy by design and default approach."[103] It claimed that DHSC "provided iterations of the DPIAs and responded constructively to feedback."[104]

---

93 https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf (p.2)

94 https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf (p.1)

95 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:21:07)

96 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:23:55)

97 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:23:55)

98 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:26:40)

99 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:22:07)

100 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:26:40)

101 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:26:40)

102 https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7 (from 15:22:07)

103 https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf (p.6)

104 https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf (p.6)

CASE STUDY C: NHS DATASTORE

During 2020, the UK government entered into contracts with a number of private technology companies to create an NHS datastore.[105] The purpose of the datastore was to collect various forms of health data from different sources across the NHS and use this data to track and analyse the spread of Covid-19.[106] It was intended that this system would be used to develop strategies for combatting the virus based on the insights produced from the data analysis. Several different datasets were used for the project, including 999 telephony activity records, PHE lab test data and NOMIS census data.[107]

The companies involved in the development of the datastore in March 2020 included Google, Faculty, Palantir and Microsoft, and they offered the following services:

- **Google**
  Google was to provide technical, advisory and other support to NHSX for the purposes of tackling Covid-19. Google agreed to provide this service without being provided access to personal data from NHSX.[108]

- **Faculty**
  The DHSC entered into a contract with Faculty to perform a number of different services. The main obligation of the company was to use healthcare data to build models that understand how the spread of Covid-19 would impact healthcare resources and also produce a dashboard that presents information pertaining to this.[109] This work envisaged the use of AI and other data science techniques to process the healthcare data.

- **Palantir**
  The NHS contracted Palantir to provide software services to collate data from different sources across the healthcare system to be used for further purposes.[110]

- **Microsoft**
  The government used Microsoft products and services to host the tools and data processed for the purposes of tackling Covid-19, such as those available on Azure.[111]

When work on the datastore commenced in March 2020, Google and Palantir provided their services for a nominal £1.[112] When the government continued work on the datastore, Palantir was awarded a £23 million contract, which was extended with a £11.5 million contract in August 2022.[113]

105 https://www.opendemocracy.net/en/ournhs/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/

106 https://transform.england.nhs.uk/key-tools-and-info/data-saves-lives/improving-health-and-care-services-for-everyone/the-nhs-covid-19-data-store-putting-data-at-the-centre-of-decision-making/

107 https://data.england.nhs.uk/covid-19/

108 https://cdn-prod.opendemocracy.net/media/documents/Google_Agreement.pdf

109 https://cdn-prod.opendemocracy.net/media/documents/Faculty_Agreement.pdf (p.13)

110 https://cdn-prod.opendemocracy.net/media/documents/Palantir_Agreements.pdf (Statement of Work)

111 https://cdn-prod.opendemocracy.net/media/documents/Microsoft_Agreements.pdf (p.5)

112 https://www.newstatesman.com/business/2022/06/peter-thiel-palantir-privatising-nhs-future

113 https://www.digitalhealth.net/2023/01/palantir-gets-11-5m-six-month-nhs-contract-extension/

NHS DATASTORE TIMELINE

28 March 2020 — The DHSC publish a blog post explaining how the NHS will be working with the private sector to develop a datastore that will support UK government decision-making around the Covid-19 pandemic.[114] That post revealed that Microsoft, Palantir, Amazon Web Services, Faculty and Google would be involved in the project.

3 April 2020 — Non-profit Foxglove submits a FOI request to the government asking for publication of the data sharing agreements concluded with the private technology companies involved in the development of the datastore, as well as any DPIAs completed for the project.[115] At the time of submission, Foxglove was unable to find a DPIA online.

15 April 2020 — The ICO announces its more relaxed approach to regulatory enforcement for the duration of the public emergency invoked by the Covid-19 pandemic.[116]

24 April 2020 — The UK government miss the deadline to respond to Foxglove's FOI request.

7 May 2020 — Foxglove teams up with openDemocracy to commence legal proceedings against the government by sending a pre-action letter requesting the release of the agreements with private technology companies for the development of the NHS datastore.[117]

14 May 2020 — The government states that it is trying to balance the "public interest" of transparency against the "commercial interests" of the companies involved regarding the FOI request, and that there would therefore be further delays responding to the request.[118]

18 May 2020 — Foxglove and openDemocracy inform the government that they intend to continue legal action in court.[119]

5 June 2020 — The government releases the contracts with the private companies involved in the development of the datastore.[120] The contracts reveal that the companies involved were granted the intellectual property rights created out of the performances of the contract (including the creation of databases), and were allowed to train their models and profit from access to NHS data. In correspondence with Foxglove, government lawyers admit this; they also claim that a subsequent, undisclosed contract amendment rectified this issue. [121]

114 https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

115 https://www.foxglove.org.uk/2020/04/06/covid-19-and-our-health-data-a-question-of-public-trust/

116 https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf

117 https://www.opendemocracy.net/en/ournhs/we-need-urgent-answers-about-massive-nhs-covid-data-deal/; https://www.foxglove.org.uk/2020/05/11/why-is-the-uk-government-hiding-its-nhs-data-deals-with-private-companies/

118 https://www.foxglove.org.uk/2020/06/05/breakthrough-uk-government-releases-nhs-covid-19-data-deals-with-big-tech/

119 https://www.foxglove.org.uk/2020/06/05/breakthrough-uk-government-releases-nhs-covid-19-data-deals-with-big-tech/

120 https://www.opendemocracy.net/en/ournhs/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/

121 https://www.foxglove.org.uk/2020/06/05/breakthrough-uk-government-releases-nhs-covid-19-data-deals-with-big-tech/

5 June 2020 — A DPIA for the programme is now available on-line;[122] it is unclear when it was published. The Data Protection Officer signed the DPIA in April 2020, and the Caldicott Guardian signed the document in May 2020.[123]

4 December 2020 — Foxglove and openDemocracy commence legal proceedings against the DHSC for the contract extension.[124]

11 December 2020 — The NHS signs a £23 million contract with Palantir to continue work on the NHS Covid-19 Datastore[125] and provide its Palantir's Foundry platform until 11 December 2022.[126]

24 February 2021 — Foxglove and openDemocracy file a judicial review of the contract with Palantir.[127]

30 March 2021 — The government commits to pausing the contract with Palantir. Specifically, the government makes three commitments: (i) to not allow Palantir to start using the Datastore for non-Covid matters without consulting the public first, (ii) to conduct new analysis to ensure compliance with data protection law prior to any expansion, and (iii) to engage with the public, via patient juries, to determine whether it is appropriate for a company like Palantir to have a long-term role in the NHS[128] [129] (at the time of writing, these commitments have not been met).

3 January 2023 — The government publishes its £11.5 million contract extension with Palantir. (the contract was signed some months prior, on 25 August 2022).[130] Under the extension, Palantir will continue to provide its Foundry platform until 11 June 2023.

16 March 2023 — Open Democracy reports that "NHS hospitals have been ordered to share people's confidential medical records with" Palantir.[131]

122 https://twitter.com/Foxglovelegal/status/1269252803601534976?s=20

123 https://www.england.nhs.uk/publication/data-protection-impact-assessment-nhs-covid-19-data-store/

124 https://www.opendemocracy.net/en/ournhs/we-need-answers-about-five-year-nhs-data-deals-big-tech/

125 https://www.contractsfinder.service.gov.uk/Notice/9233a767-bd2b-49eb-9c57-310bb2e259e0

126 https://www.england.nhs.uk/blog/data-integration-driving-improvements-in-patient-care/

127 https://www.theregister.com/2021/02/24/nhs_palantir_judicial_review/

128 https://www.opendemocracy.net/en/ournhs/weve-won-our-lawsuit-over-matt-hancocks-23m-nhs-data-deal-with-palantir/

129 https://www.foxglove.org.uk/2021/04/01/success-uk-government-concedes-lawsuit-over-23m-nhs-data-deal-with-controversial-us-tech-corporation-palantir/

130 https://www.contractsfinder.service.gov.uk/notice/2cf9dde2-3991-4b41-8971-a9ee7ec432e2

131 https://www.opendemocracy.net/en/palantir-peter-thiel-nhs-england-foundry-faster-data-flows/

DATA PROTECTION ISSUES WITH THE NHS DATASTORE

Legal basis for processing

Under Article 6(1) of the GDPR, the processing of personal data requires an appropriate lawful basis and under Article 9(1), the processing of special categories data – such as health data as is the case with the NHS datastore – cannot be processed unless one of the exceptions under Article 9(2) applies. As the ICO's Data Sharing Code of Practice states, without a lawful basis of processing, the controller will be in breach of the GDPR and data protection law.[132] It is not apparent from the contracts with Faculty, Palantir and Microsoft what legal basis the government relied on to provide the companies with such data. In a DPIA published after the contracts with Faculty and others were signed, NHS England confirmed that the legal basis being relied on was Article 6(1)(e), which allows for processing that is "necessary for the performance of a task carried out in the public interest."[133]

Due diligence and data sharing with private companies

Under Article 28(1) of the GDPR, data controllers are required to ensure that their processors provide sufficient guarantees to implement the appropriate technical and organisational measures to comply with the Regulation. This obligation applies both before entering into a data processing agreement with the processor and during the duration of that agreement. Accordingly, before procuring the services of Faculty, Palantir and Microsoft, the UK government would have been required to carry out a risk assessment of these vendors to ensure that relevant data protection requirements could be met, including around security and the potential sharing of data with subprocessors. In doing so, the reputation of the processor may be a relevant factor to consider.[134] For example, in November 2015, the Royal Free London NHS Foundation Trust partnered with Google DeepMind to develop software to detect acute kidney injury using the sensitive medical data of millions of the Trust's patients; according to the ICO, such a transfer of data was not compliant with the Data Protection Act 1998, including the principles of lawfulness fairness and transparency, as well as data minimisation.[135]

This connects to a wider issue regarding public procurement. The public health emergency triggered by the Covid-19 pandemic required governments to rely on private organisations to acquire the necessary resources. However, public procurement of these services did not follow the usual due diligence processes, and governments used expedited processes to assess and procure services from the private sector. While this could be justified,[136] in the context of data processing agreements under Article 28(3) of the GDPR, the controller must still refrain from clauses and terms that may be contradictory to data protection law.[137] Even amidst a public health emergency, the UK government is not relieved of its duty to make reasonable decisions around expedited public procurement processes,[138] which includes issues pertaining to data protection requirements.

In addition, the processors used for the processing operation must be disclosed in a privacy notice provided to data subjects. This is required by Articles 5(1)(a) and 13(1)(e) of the GDPR, as well as the ICO's Data Sharing Code of Practice (which was in draft form at the time that the original contracts with Faculty and others were signed). This

132 https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/lawful-basis-for-sharing-personal-data/

133 https://www.england.nhs.uk/wp-content/uploads/2022/02/data-protection-impact-assessment-nhs-covid-datastore.pdf

134 https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (para. 97)

135 https://ico.org.uk/media/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf

136 https://www.bailii.org/ew/cases/EWHC/TCC/2022/46.pdf (para. 462)

137 https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (para. 110)

138 https://www.bailii.org/ew/cases/EWHC/TCC/2022/46.pdf (para. 478)

includes the purpose of the data being shared with these processors, their respective roles and how data subjects can exercise their rights under the GDPR. Such transparency around the datastore has been lacking ever since work on it first started in March 2020.

International data transfers

Under Chapter V of the GDPR, there are three mechanisms that can be used for transfers of personal data from the EU to third countries (i.e. non EU Member States). This includes (i) an adequacy decision by the European Commission under Article 45, whereby the Commission deems a third country to have a data protection framework that is essentially equivalent to that in the EU under the GDPR and the EU Charter, (ii) a set of transfer tools that provide appropriate safeguards under Article 46, and (iii) a derogation under Article 45. For the contract with Palantir, the UK government included in an annex a set of standard contractual clauses (SCCs) for data transfers, which is one of the Article 46 transfer tools.[139]

In July 2020, the Court of Justice of the European Union (CJEU) handed down its judgment in Schrems II and made a number of significant stipulations regarding data transfers to the US.[140] Firstly, it ruled that the adequacy decision in favour of the US, known as the Privacy Shield, was declared unlawful and void and therefore could no longer be used for US data transfers.[141] Secondly, when using SCCs under Article 46 for transfers, the controller must carry out a transfer impact assessment (TIA) to assess the laws of the third country that the data are being transferred to.[142]

Even though Palantir reportedly shifted all UK data processing operations out of the US in 2021,[143] including processing for the NHS, the government would have been required to conduct a TIA for data transfers to the US before this shift by Palantir. In particular, this assessment should have been completed prior to concluding the agreement with Palantir. A similar exercise would have needed to be carried out for the contract with Microsoft if the use of its services involved data transfers to third countries.

Lack of DPIA

The UK government's contracts for the creation of the datastore included, among other things, the development of AI tools to track and analyse the spread of Covid-19 using a range of health data. This would have likely necessitated the completion of a DPIA prior to processing; Article 35(3)(b) of the GDPR requires that large-scale processing of sensitive data, which patient data would constitute under Article 9(1), requires a DPIA. The NHS eventually released a DPIA on the NHS Datastore in 2022,[144] however such an assessment would have needed to be completed prior to the processing of personal data. It is unclear whether a DPIA was completed at the time that the contracts with Faculty and others were agreed prior to development of the datastore.

---

139 https://cdn-prod.opendemocracy.net/media/documents/Palantir_Agreements.pdf

140 https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=159429

141 https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=159429 (para. 168-201)

142 Ibid. (para. 134)

143 https://www.reuters.com/technology/palantir-localize-uk-data-operations-privacy-regulations-tighten-2021-12-17/

144 https://www.england.nhs.uk/wp-content/uploads/2022/02/data-protection-impact-assessment-nhs-covid-datastore.pdf

NHS FEDERATED DATA PLATFORM

Palantir's relationship with the NHS is ongoing, and it is believed to be a strong contender to win the NHS' Federated Data Platform (FDP) contract. Foxglove has described the FDP, which is currently in the procurement process, as the 'NHS Data Grab 2'.[145]

The FDP will be a software platform that "will enable NHS organisations to bring together operational data – currently stored in separate systems – to support staff to access the information they need in one safe and secure environment so that they are better able to coordinate, plan and deliver high quality care".[146] Each hospital trust and integrated care system will have their own platforms to facilitate collaboration with others that also have access to the system. The idea for the FDP has its origins in a DHSC policy published in June 2022, which details the government's ambitions to improve the data analytics eco-system within the NHS.[147] Palantir is tipped to win the contract, and has hired senior NHS officials in preparation, including the former NHS head of artificial intelligence and the former deputy to NHS England's data chief, who is responsible for the FDP contract and Palantir's previous contracts with the NHS.[148]

Timeline

April 2022: The government announced the development of the Federated Data Platform. The estimated £240 million contract comprised of two parts: the provisioning of services for the development of a central data platform collating different sources of NHS data, and the development of privacy enhancing technology.[149]

6 June 2022 (the original estimated date of publication of the FDP contract notice): The contract notice is not published.

July 2022: The government stated that it would not be carrying out a public consultation prior to entering into contracts for the development of the FDP.[150]

25 July 2022: The procurement notice was modified, increasing the estimated contract value to £360 million and changing the estimated publication date to 5 September.[151] The notice maintained the intention to procure privacy enhancing technology.

5 September 2022 (the estimated date of publication): the contract notice was not published.

3 January 2023: The government published the £11.5 million extension of its NHS Datastore contract with Palantir (the contract was signed some months prior, on 25 August 2022).[152] Under the extension, Palantir will provide its Foundry platform until 11 June 2023 while the procurement of the new FDP is underway and support transition to the new service.[153]

10 January 2023: The government published the first contract notice for FDP, with an estimated total value of £360 million for 5 years. There will be an additional option to extend, with a total estimated value of up to £480 million over the contract period.[154]

145 https://www.foxglove.org.uk/2022/09/30/doctors-not-dashboards-360m-palantir/

146 https://www.england.nhs.uk/blog/better-insights-better-decisions-better-health/

147 https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data/data-saves-lives-reshaping-health-and-social-care-with-data#improving-trust-in-the-health-and-care-systems-use-of-data

148 https://www.ft.com/content/3f6f24f8-9e5c-42c3-8ae6-bfef5f953524

149 https://www.find-tender.service.gov.uk/Notice/008755-2022

150 https://www.theregister.com/2022/07/20/nhs_data_platform_consultation/

151 https://www.find-tender.service.gov.uk/Notice/020196-2022?origin=SearchResults&p=1

152 https://www.contractsfinder.service.gov.uk/notice/2cf9dde2-3991-4b41-8971-a9ee7ec432e2

153 https://www.contractsfinder.service.gov.uk/notice/2cf9dde2-3991-4b41-8971-a9ee7ec432e2

154 https://www.find-tender.service.gov.uk/Notice/000669-2023

ICO RESPONSE TO THE NHS DATASTORE

Despite the clear risk posed to the safety of public health data by the involvement of Palantir and other large corporations, it is unclear what involvement, if any, the ICO had with the NHS Datastore. In the DPIA published for the programme, the section titled 'Advice of the ICO' has been left blank, suggesting that the ICO was not as closely involved in the Datastore as it was for the contact tracing app.[155]

A response to an FOI request published in November 2022 gives some indication of the ICO's involvement in the FDP.[156] The ICO confirmed that members of staff from the Relationship Management Service have had discussions with NHS Digital and NHS England regarding the platform, although these have been initial discussions involving high level details.

"This [FDP] proposal is still in the 'overarching high level Information Governance policy' formulation stage and has not reached the stage where for example, the risk assessment has been completed and determined that there is unmitigated risk, at which point they would move to consult with us under Art 36(5) – prior consultation on their Data Protection Impact Assessment. We do not know at this stage what the outcome of the risk assessment will be and whether the threshold for prior consultation will be met."

As such, the ICO has not been consulted on the initiative nor "issued any advice or exercised any regulatory powers."[157]

The response mentions that the ICO became aware of proposals for a FDP during its engagement on the Health and Care 2022 and the Data Save Lives Data Strategy from DHSC. In October, both NHS England and ICO started more formal engagements on these matters and intend to have ongoing monthly meetings in the future. However, as the timeline above indicates, an information notice for the FDP was published in April. It would appear that the ICO is only superficially involved, and does not plan a proactive approach with the FDP.

155 https://www.england.nhs.uk/wp-content/uploads/2022/02/data-protection-impact-assessment-nhs-covid-datastore.pdf

156 https://ico.org.uk/media/about-the-ico/disclosure-log/4022927/ic-202206-r1b9-response.pdf

157 https://ico.org.uk/media/about-the-ico/disclosure-log/4022927/ic-202206-r1b9-response.pdf

3 THE ICO IN CONTEXT

The ICO's regulatory approach to Covid-19 was communicated poorly. Initially, it appeared that it had ceased important regulatory functions all together when, in a letter responding to a data protection complaint, the ICO wrote:

"Unfortunately, I am not able to write to [the company in question] for further information about your complaint and their information rights practices, at present…This is because, as you are aware, the coronavirus pandemic is putting unprecedented pressure on all organisations and a great many are either suspending activity or having to prioritise resources…We have therefore decided not to take forward any complaints that require organisations to take action or respond to enquiries from us until the situation improves."[158]

Following a complaint by ORG and reporting by Wired, the ICO clarified that it was still pursuing investigations, and had only paused activity for less than 10 per cent of cases and investigations. In a public statement in April 2020,[159] the ICO stated it would "balance the benefits to the public and the dissuasive effect of taking regulatory action against the effect of doing so on regulated organisations, taking into account the particular challenges being faced by organisations and the UK economy."[160]

This approach, as well as the shortcomings identified in the above case studies, led to the following failings.

3.1 THE ICO WAS ABSENT FROM DATA PROTECTION CONVERSATIONS WHEN IT WAS NEEDED MOST

The ICO faded into the background of data protection conversations when it should have been a key player, leaving civil society and the public to fill the regulatory and oversight gap and ask challenging questions. The regulator failed to step up at a time when public trust was essential for the success of health programmes that could limit the spread of the pandemic and save lives.

The ICO generally failed to provide any meaningful comment that could have driven the government to make the right decisions or to hold them to account for their mistakes. When the ICO did intervene, this was usually the outcome of public pressure: for instance, with Test and Trace, the ICO conducted a consensual audit of the programme only after ORG 's legal action against the Test and Trace programme and the DHSC. Likewise, Foxglove and Open Democracy stepped in with the NHS Datastore, whereas the ICO is still largely absent on the subject.

In comparison, Datatilsynet and CNIL, the data protection authorities in Norway and France, were central to the data protection conversations in their countries and were willing to exercise their regulatory powers to move from advice to intervention. Datatilsynet's temporary ban on Norway's contact tracing app, which it found to be a disproportionate intervention in users' fundamental rights, helped shape the trajectory of app's

158 Letter quoted in Wired. https://www.wired.co.uk/article/ico-data-protection-coronavirus

159 https://web.archive.org/web/20220809101430/https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/04/how-we-will-regulate-during-coronavirus/

160 https://web.archive.org/web/20220901055950/https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf

development, and the launch of a new version. In the UK, the ICO said that it was consulted by the government but "did not have a seat at the design table". The ICO failed to publicly comment on the delayed publication of the first DPIA or other data protection concerns raised by first version of the contact tracing app.

3.2 THE ICO WAS ILL-PREPARED TO DEAL WITH AN EMERGENCY COMPARED TO OTHER UK REGULATORS

The ICO's reluctance to take enforcement action is at odds with the approaches of other UK regulators. In general, while other UK regulators clearly emphasised regulatory continuity and individuals' welfare as their priority during the pandemic, the ICO's approach focused more heavily on relaxing regulatory oversight on businesses.[161] Additionally, the Financial Conduct Authority (FCA) recognised the need to learn from their initial pandemic response and created strong protocols for future emergency situations.

The Covid-19 crisis has shown that regulators must be prepared to apply legal safeguards to protect the public even during challenging circumstances. As the Commissioner rightly pointed out in her reflections that followed the start of the pandemic, the UK GDPR provided transparency, accountability, and the safeguards the public needed in a time of emergency.[162] However, the Commissioner did not follow in practice what she praised in principle. While there is no fault in acknowledging that public and private organisations were operating under difficult circumstances, the ICO's approach was timid and lax, avoiding strong enforcement even when the government's clear breaches of data protection law were causing harm to citizens.

3.3 EUROPEAN DATA PROTECTION AGENCIES

NORWAY'S DATATILSYNET

Datatilsynet is the data protection supervisory authority (DPA) for Norway. During the pandemic, Datatilsynet prioritised work and investigations related to Covid-19 with a particular focus on the national contact tracing app.[163]

Action taken against Norway's contact tracing app

In April 2020, the Norwegian Institute of Public Health, a Norwegian government agency, launched a national contact tracing app called Smittestopp ('Infection Stop').[164] Later that same month, the Datatilsynet published its opinion on Smittestopp.[165] It stated that it was following the developments of the app closely and warned about potential excessive intrusions of privacy. In particular, the DPA pointed out that, even if the use of the app is voluntary, monitoring a person's movements constitutes an invasion of privacy and users should have the ability to choose which functions or features of the app that they want to provide their personal data for.

On 12 June 2020, the Datatilsynet issued a decision for the temporary ban on the processing of personal data by Smittestopp.[166] The DPA found that the app was in breach of the transparency principle, the data minimisation principle and the right of access

161 https://www.dataguidance.com/news/uk-ico-publishes-guidance-regulatory-approach-during

162 https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf

163 https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsrapport-for-2020/

164 https://www.thelocal.no/20200416/norway-launches-smittestop-app-to-track-coronavirus-cases/

165 https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/starter-kontroll-av-smittestopp/

166 https://www.datatilsynet.no/en/news/2020/temporary-suspension-of-the-norwegian-covid-19-contact-tracing-app/

under Articles 5(1)(a), 5(1)(c) and 15 of the GDPR, respectively.[167] As such, the app was deemed to not be "a proportionate intervention in the users' fundamental rights to data protection."[168] The temporary ban did provide the Norwegian Institute of Public Health with the opportunity to bring the processing in compliance with the GDPR. After the decision, the Health Institute stopped processing operations for the app and deleted the data collected.[169]

Later that year in December, the Public Health Institute launched a new version of Smitestopp, which made use of the decentralised contact tracing model provided by the Google/Apple Exposure Notification API.[170] The Datatilsynet was closely involved in the development of the app, including on the risk analysis, and was satisfied that it was more privacy-friendly than its predecessor.

FRANCE'S CNIL

The Commission Nationale Informatique et des Libertés (CNIL) is the data protection supervisory authority for France. In response to Covid-19, CNIL made some adjustments to its regulatory approach. It prioritised complaints relating to Covid-19 and closely monitored measures implemented by public authorities in response to the pandemic, including contact tracing apps and the use of surveillance drones.[171] The regulator also temporarily suspendeded on-site inspections whilst France was under a national lockdown, during which investigations were carried out remotely. However, for 2020, the CNIL managed to conduct 247 investigations, 72 of which involved on-site inspections carried out after lockdown measures were eased. It imposed 14 sanctions, which included 11 fines amounting to almost €200 million.[172]

In May 2020, when France extended the state of emergency originally declared in March, it also passed a decree providing a basis for Covid-related measures involving the collection and analysis of health data.[173] Prior to implementing these initiatives, public authorities were required to draft separate decrees authorising each measure and submit those to the CNIL for comment. The regulator interpreted this obligation broadly, requesting that it receive any DPIAs carried out for these measures and "be informed of the conditions of their deployment."[174]

Response to France's contact tracing app

In June 2020, Santé Publique France, the French Public Health authority, released the StopCOVID contact tracing app.[175] The CNIL was closely involved in the development of StopCOVID. In April 2020, the French government sought the opinion of the CNIL regarding the development of the app to ensure that its data processing was compliant with the GDPR and French data protection law.[176] In that opinion, the CNIL found that subject to certain conditions such as sufficient transparency and an appropriate legal basis, the StopCOVID app would be compliant with the applicable law. In May 2020, the French

167 https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/02058

168 https://www.datatilsynet.no/en/news/2020/temporary-suspension-of-the-norwegian-covid-19-contact-tracing-app/

169 https://www.fhi.no/en/news/2022/fhi-legger-ned-smittestopp/; https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en

170 https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-smittestopp-lansert/

171 https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2020

172 https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2020

173 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041865244/

174 https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_8_may_2020_delivering_an_opin-ion_on_a_draft_decree_mentioned_in_article_6_of_the_draft_law_extending_the_state_of_health_emergency.pdf (p.3)

175 https://techcrunch.com/2020/06/02/france-releases-contact-tracing-app-stopcovid-on-android/

176 https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_april_24_2020_delivering_an_opinion_on_a_proposed_mobile_application_called_stopcovid.pdf

government requested CNIL's opinion on a draft decree providing the legal basis of the app;[177] this was requested after it was announced that the app had entered its testing phase.[178] This May opinion essentially approved the implementation of StopCOVID while offering additional amendments to the draft decree to ensure compliance with the GDPR.

After the launch of StopCOVID, the CNIL initiated checks to ensure the proper functioning of the app to verify that data processing was compliant with data protection legislation.[179] After conducting these checks, the CNIL found a number of infringements with the GDPR, such as failing to provide an adequate description of data processing operations in the updated DPIA for the app.[180] In November 2020, it confirmed that the government sending SMS messages to subscribers of telephone operators in France about using TousAntiCovid was lawful.[181]

Response to the use of drones

After France went into lockdown in March 2020, it was reported in the press that police forces were using drones equipped with cameras to ensure compliance with lockdown measures by the public. After the CNIL received no response to its initial inquiries lodged with the Ministry for Interior on the matter, the regulator commenced an investigation on 7 May 2020 to determine whether the use of the drones by police was compliant with the GDPR and French data protection law.[182]

On 18 May, the Conseil d'État (the French Administrative Supreme Court) handed down its judgment on the use of drones by the police after legal proceedings were brought by La Quadrature du Net challenging the legality of such measures.[183] The Court found that the use of the drones was unlawful and ordered for the immediate cessation of their use.

Separately, as part of its own investigation, the CNIL visited the premises of the police force to carry out on-site checks. This involved a demonstration of the drone surveillance capabilities via test flights. In October 2020, the appointed rapporteur for the case produced a report detailing the infringements of law resulting from the use of the drones. The Ministry argued that the drones were equipped with technology that blurred the faces of those captured in the drone footage, and that therefore their data was anonymised and not subject to data protection law. The CNIL noted that the blurring technique was only applied after the collection of the images and thus did not ensure that persons captured by the drone could not be identified using the images. Accordingly, the CNIL found that the police had been using drones without an appropriate legal basis and sanctioned the Ministry under an official decision published in January 2021.[184]

177 https://www.cnil.fr/sites/default/files/atoms/files/deliberation_ndeg_2020-056_from_25_may_2020_delivering_an_opinion_on_a_draft_decree_relating_to_the_mobile_application_known_as_stopcovid.pdf

178 https://twitter.com/cedric_o/status/1257567804401897474

179 https://www.cnil.fr/fr/si-dep-contact-covid-et-stopcovid-la-cnil-lance-sa-campagne-de-controles

180 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042125452/

181 https://www.cnil.fr/fr/tousanticovid-le-gouvernement-sadresse-aux-abonnes-des-operateurs-telephoniques

182 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042960768

183 https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-05-18/440442

184 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042960768

3.4 OTHER UK REGULATORS

FINANCIAL CONDUCT AUTHORITY

The FCA is the UK's regulator for the financial services industry. The regulator is responsible for protecting consumers, keeping the financial industry stable, and promoting healthy competition between financial service providers. During the pandemic, the FCA transitioned to working from home but continued to operate as normal.

The FCA adjusted its supervisory approach and regulatory focus to account for the impact of the Covid-19 pandemic, with a strong focus on protecting the welfare of consumers. The FCA's Business Plan for 2020/21 highlighted the regulator's "continued focus on firms' treatment of vulnerable and potentially vulnerable customers, a group that is likely to grow significantly as a result of the Covid-19 outbreak."[185] The organisation also highlighted key internal plans, stating that it planned "to update its entire regulatory system to enable it to act faster in emergency situations, so that firms and individuals can be removed from the regulated sector promptly when required."[186]

THE COMPETITION AND MARKETS AUTHORITY

The Competition and Markets Authority (CMA) is the UK's competition regulator responsible for enforcing against anti-competitive behaviour in the economy. During the pandemic, the CMA updated its working practices. On 18 March 2020, it announced that certain precautions would be implemented, taking into account public health advice.[187] This included requiring all staff to work from home and conducting all meetings remotely. However, the CMA confirmed that any binding statutory deadlines would continue to "apply to a significant proportion of the CMA's work" and that it intended to "continue progressing its cases, making decisions and meeting deadlines."[188]

In addition, the CMA recognised its role in responding to new and expanded areas of concern during the pandemic. It established a Covid-19 taskforce to identify and act on businesses exploiting the public health crisis, for instance by "charging excessive prices or making misleading claims about their products."[189] With this taskforce, the CMA committed to taking enforcement action against firms where there was evidence of competition or consumer law being breached.[190] As an example: in December 2020, the CMA focus on the holiday accommodation and travel sectors led to LoveHolidays[191] committing to a payout of over £18 million to customers whose holidays were cancelled due to coronavirus. [192]

185 https://www.pinsentmasons.com/out-law/analysis/fca-business-plan-coronavirus-impact

186 Ibid.

187 https://www.gov.uk/government/news/covid-19-cma-working-arrangements

188 https://www.gov.uk/government/news/covid-19-cma-working-arrangements

189 https://www.gov.uk/government/news/cma-launches-covid-19-taskforce

190 https://www.gov.uk/government/news/cma-launches-covid-19-taskforce

191 https://www.gov.uk/government/news/update-on-cma-covid-19-taskforce

192 https://www.gov.uk/government/news/loveholidays-to-refund-over-18-million-for-cancelled-holidays

4 HOW THE DPDI BILL WILL UNDERMINE DATA PROTECTION IN THE UK

The Data Protection and Digital Information (DPDI) Bill is expected to replace the Data Protection Act 2018, and reform the GDPR. There are a number of ways in which the reforms to the GDPR proposed in the DPDI Bill may exacerbate shortcomings and concerns raised by the three Covid-19 health surveillance case studies.

During the pandemic, the government disregarded data protection law by ignoring the DHSC's failure to produce a DPIA, boasting that they would not be held back by bureaucracy.[193] Further, the consultation that led to the formulation of the DPDI Bill systematically ignored critical voices and excluded Civil Society from meaningful engagement with the consultation process.[194] The result is, as recently denounced by civil society, a Bill that would weaken data subjects' rights, water down accountability requirements, further reduce the independence of the ICO, and empower the Secretary of State with undemocratic controls over data protection.[195]

4.1 THE DPDI BILL WILL WEAKEN THE UK GDPR'S ACCOUNTABILITY FRAMEWORK

REMOVAL OF THE REQUIREMENT TO CONDUCT DPIAS

The DPDI Bill will introduce a range of changes to the Article 35 requirement to carry out a Data Protection Impact Assessment (DPIA). Notably, Clause 17 removes the requirement to carry out DPIAs and replaces it with an "assessment of high-risk processing", while Clause 18 removes the requirement of prior-consultation with the Commissioner for processing operations whose risks cannot be mitigated. Key issues with these changes include:

- Requirements for what DPIAs must contain will be less prescriptive, likely leading to shorter, less comprehensive assessments.
- The requirement to consult representatives of data subjects is removed.
- The list of circumstances in which a DPIA is assumed to be required is removed, leaving controllers with more latitude to decide whether to carry one out.
- The requirement to consult the Commissioner where a DPIA identifies high risks to data subjects is removed.

These changes are likely to lead to fewer DPIAs being conducted, and, where they are conducted, DPIAs will contain less detail and be less informed about data subjects' views. DPIAs are also much less likely to be referred to the ICO (although it is unclear how common this practice is even under the current regime).

193 https://twitter.com/OpenRightsGroup/status/1285260608875700225?s=20

194 https://techmonitor.ai/policy/privacy-and-data-protection/data-reform-bill-consultation-dcms-nadine-dorries

195 https://www.openrightsgroup.org/app/uploads/2023/03/DPDI-Bill-UK-civil-society-letter.pdf

REMOVAL OF THE REQUIREMENT TO KEEP RECORDS OF PROCESSING ACTIVITIES

Clause 15 will introduce a new Article 30A UK GDPR that will exempt organisations from maintaining record of processing activities (ROPA) unless the organisation carries out data processing that "is likely to result in a high risk to the rights and freedoms of individuals". Further, the existing requirement for a comprehensive ROPA will be replaced with a less extensive 'appropriate records' even in high-risk scenarios. This will lead to fewer and less comprehensive records of controllers' processing.

Impact of these changes

The three Covid-19 health programmes described in this report clearly required DPIAs under the current GDPR regime: they met the criteria in the current Article 35(3) GDPR. Under the new Bill, it will be much less clear whether health surveillance processing like this will require a DPIA; the public authorities proposing it will have more latitude to decide for themselves whether to carry one out. Over time, as fewer DPIAs are carried out and referred to the ICO, it may also be expected that the regulator's institutional knowledge and capacity to assess complex and novel processing in health surveillance will be diminished.

DPIA and ROPA requirements were key mechanisms of accountability for the three Covid-19 health programmes (in particular where DHSC was forced to admit that T&T was unlawful due to its failure to conduct a prior DPIA). The GDPR's accountability framework is what helps civil society understand and challenge national-scale sensitive processing. By way of example, civil society will be reliant on the GDPR accountability framework to understand how providers such as Palantir are proposed to be given further - and longer-term - access to national datasets as part of the NHS Federated Data Platform, and the measures being put in place to ensure that data is not used for purposes that lack public consent. The DPDI Bill's reforms look set to significantly undermine the accountability framework, which will likely further enable health surveillance and make it less susceptible to challenge.

REMOVAL OF THE REQUIREMENT TO CONDUCT LEGITIMATE INTEREST ASSESSMENTS AND COMPATIBILITY TESTS

Clause 5 would introduce new Article 6(1)ae, which would allow the Secretary of State to exempt private organisations from carrying out a Legitimate Interest Assessment (LIA, also know as balancing test) when using personal data for a given purpose.

Further, Clause 6 would introduce new Article 8A UK GDPR, which would allow the Secretary of State to exempt public or private organisations from assessing and limiting data processing for new purposes that aren't 'compatible' with the purpose for which data was collected (i.e. not in breach of the principle of purpose limitation).

LIAs are important safeguards and accountability measures. They require organisations to think about the processing they intend to do and the impact on people at the outset, and allow individuals and regulators to scrutinise the legitimacy of such decisions. Likewise, purpose limitation is a key driver of public trust and safeguard against abuses.

Impact of these changes

The three Covid-19 programmes all involved the collection of very large amounts of data into new datasets that had never before existed in the UK. This collection has been justified by reference to the pandemic. But the temptation to use the data for other purposes once collected will be strong.

Under the current regime, a controller wishing to carry out processing for a new purpose using a health surveillance dataset needs to satisfy the principle of purpose limitation. The reforms will allow them to side-step this requirement in many public sector-adjacent contexts.

For example, a public authority might look to reuse health surveillance data for the purposes of crime detection[196]. It could well be argued under the current regime that such reuse would breach the principle of purpose limitation, but this ground of challenge would not be available under the reformed UK GDPR[197].

Finally, these reforms would make it more difficult to scrutinise the legitimacy of data processing, while increasing the legal scope for data collected through health surveillance programmes (which may enjoy support from data subjects) to be reused in markedly different contexts and in ways that data subjects do not expect and would not support. The principle of purpose limitation, set to be weakened by the DPDI Bill, would be one important way of challenging any use by providers such as Palantir of data originally collected in a health context for law or immigration enforcement purposes.

4.2 THE DPDI BILL WILL WATER DOWN THE STATUTORY FUNCTION OF THE ICO AND THREATEN ITS INDEPENDENCE

CHANGES TO THE STATUTORY OBJECTIVE OF THE ICO

The DPDI Bill will shift the focus of the ICO from protecting the public to protecting businesses and government interests. Clause 27 of the DPDI Bill would insert new §120A and 120B to the Data Protection Act 2018. Critically, it would require the ICO to consider the desirability of promoting innovation, and competition, and the importance of the prevention, investigation, detection and prosecution of criminal offences as well as the need to safeguard public security and national security.

Impact of these changes

Recital 129 of the UK GDPR clearly states that the Commissioner must exercise their powers "impartially, fairly and within a reasonable time" and "in view of ensuring compliance with this Regulation". By introducing a new, ambivalent principal objective and a list of secondary ones, the DPDI Bill would only complicate and reduce clarity over what the Commissioner is expected to do.

In turn, this is bound to further reduce the effectiveness of the ICO as a regulator: as pointed out by the Institute for government, "clarity of roles and responsibilities is the most important factor for effectiveness" of arms-length bodies.[198]

196 This was explicitly envisaged in the context of Test and Trace. Under the Health Protection (Coronavirus, Restrictions) (Self-Isolation) (England) Regulations 2020 (no longer in force), data collected for test and trace could be given to the police for the purposes of enforcement and prosecution

197 Note that the new processing would still need to comply with the rest of the requirements of the GDPR even if it is considered 'compatible' with the original purpose.

198 Read before burning, p. 33

NEW MINISTERIAL POWERS TO INTERFERE WITH THE FUNCTIONING OF THE ICO

The Bill will give the Secretary of State new powers to issue instructions to the ICO and to exercise control over some of its functions. Clause 28 of the DPDI Bill would insert new §120E and 120F to the Data Protection Act 2018, which allow the Secretary of State to designate strategic priorities for the Commissioner to 'have regard to' in carrying out his or her functions, except when they relate to a particular person, case or investigation.

Clause 31 of the DPDI Bill would insert new §124D to the Data Protection Act 2018, which would establish a new power for the Secretary of State to review and either approve or stop the ICO from submitting a Code of Practice to Parliament.

Clause 33 of the DPDI Bill would insert new §139A to the Data Protection Act 2018, which would establish a new duty for the Commissioner to "prepare and publish an analysis of the Commissioner's performance using key performance indicators". KPIs are defined as "factors by reference to which the Commissioner's performance can be measured most effectively".

Impact of these changes

The government will entrench their power to exercise political influence over the Information Commissioner. Even if the ICO remained independent in relation to investigations, the ICO's focus could be drawn away from areas where the Secretary of State would prefer less scrutiny (for example, the area of health surveillance), thus reducing standards of enforcement and standard-setting in those areas.

Further, the Commissioner would be required to seek government approval and collaboration when issuing Codes of Practice, and would be open to a review of the Commissioner's operations not on the basis of whether his or her actions have been rational, lawful or proportionate, but on the basis of undefined and potentially arbitrary key performance indicators. The government could also use their power to issue a statement of strategic priorities to politicise those KPIs.

4.3 THE DPDI BILL WILL DISEMPOWER THE PUBLIC AND REDUCE SCRUTINY OVER DATA GOVERNANCE AND PRACTICES

LIMITATIONS ON THE EXERCISE OF DATA SUBJECT RIGHTS

Clause 7 of the DPDI Bill would insert a new Article 12A into the UK GDPR which allows controllers to refuse the exercise of data subject rights in Articles 15 to 22 and 34 where the exercise is 'vexatious or excessive'. These rights include the right of access, right to erasure, and right to object to processing.

'Vexatious or excessive' replaces the current test in the GDPR under which requests can only be refused or charged for where they are 'manifestly unfounded or excessive'. The intention of the change appears to be to afford controllers more discretion in refusing or charging for requests[199].

In tandem, the DPDI Bill introduces a new Article 12B UK GDPR, which gives data controllers greater flexibility in delaying responding to the exercise of data subject rights. Clauses 39 and 40 would also introduce new sections (164A and B, and 165A and B) into the Data Protection Act 2018. The combined effect is that data subjects must first complain to the data controller before complaining to the Information Commission. The practical

199 See https://www.awo.agency/files/Briefing-Paper-3-Impact-on-Data-Rights.pdf for a more comprehensive explanation of the changes.

effect of this – in combination with the likely increase in satellite complaints about whether exercise of rights is 'vexatious or excessive' is that many complaints would take 20 months or longer to resolve.[200]

Impact of these changes

Data subject rights are at the heart of the GDPR. Data protection law recognises that processing is often invisible or poorly understood by data subjects, making the right of access particularly fundamental to the protection of privacy. Whilst in theory the burden of demonstrating that a request is invalid is on the controller, in practice controllers decide whether to action a request, meaning it is data subjects who have to prove their right to access, objection, and erasure.

This is evident in relation to the programme case studies. Health surveillance processing will often be invisible, poorly understood, or carried out otherwise than on the basis of data subjects' consent. While none of this is necessarily unlawful, it clearly shows the importance of data subjects being able to exercise their rights in respect of health surveillance processing. By way of example, it will be crucial that data subjects can easily access copies of their personal data held in the Datastore or NHS Federated Data Platform. It is only through this access that individuals can hope to understand the new 'view' that the health surveillance project has provided not only to the government, but also to its private sector processors such as Palantir.

LIMITATIONS ON THE RIGHT TO LODGE A COMPLAINT

The proposed data reforms will undermine the rights of data subjects, who will be less informed and less empowered to challenge health surveillance processing.

Clause 40 of the DPDI Bill would insert new §165A to the Data Protection Act 2018, according to which the Commissioner would have discretion to refuse to act upon a Complaint, if the complainant didn't try to resolve the infringement of their rights with the relevant Controller and at least 45 days have passed since then.

Impact of these changes

The ICO already has a poor track record in acting upon complaints. This change will make it even more difficult to successfully get redress when submitting a complaint. In the context of the Covid-19 case-studies, lack of action by the ICO led to important public programmes being run in breach of key data protection provisions, and forced civil society and the wider public to mobilise themselves to address shortcomings in regulatory oversight .

By expanding the Commissioner's discretion to refuse to act upon a given complaint, the DPDI Bill would further reduce accountability over the ICO's objective and impartial conduct in the context of investigations and complaints' procedure.

200 Ibid.

5 RECOMMENDATIONS

5.1 RECOMMENDATIONS FOR GOVERNMENT

DROP THE DPDI BILL

The Covid-19 pandemic has proven that the UK data protection framework is a flexible regime, that allows the deployment of important public health programmes subject to appropriate safeguards. As the previous commissioner pointed out in her reflections that followed the pandemic, UK GDPR principles provided flexibility alongside "the safeguards the public still expected to be in place – transparency, fairness, necessity, and proportionality – backed by an independent regulator to hold organisations to account".[201]

However, the DPDI Bill would remove or render accountability requirements meaningless, further exacerbating the data protection issues identified in this report. The DPDI Bill would also weaken the UK's data protection infrastructure, leaving civil society and the public with fewer tools with which to demand accountability. Finally, the Bill does nothing to encourage increased enforcement action by the ICO and instead threatens to politicise the regulator, allowing the Secretary of State to set strategic priorities for the Commissioner. The result is, as recently denounced by civil society, a Bill that would weaken data subjects' rights, water down accountability requirements, further reduce the independence of the ICO, and empower the Secretary of State with undemocratic controls over data protection.[202] The government should drop the DPDI Bill and bring data protection reform legislation back to the design stage.

The government should ensure that data protection experts, civil society and ordinary citizens are thoroughly consulted in the development of new data reform legislation. Evidence to inform data protection policy-making could be based upon the findings from the Joint Committee on Human Rights report on "The Right to Privacy (Article 8) and the Digital Revolution". Proposals in that report to strengthen consent requirements and legitimate interest assessments, to implement the UN guiding principles on Business and Human Rights, and to promote a stronger enforcement of data protection legislation should be developed into a coherent legislative proposal. Any new legislation should consider the following recommendations:

201 https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf

202 https://www.openrightsgroup.org/app/uploads/2023/03/DPDI-Bill-UK-civil-society-letter.pdf

REQUIRE PUBLIC AND PRIVATE ORGANISATIONS TO PUBLISH KEY ACCOUNTABILITY DOCUMENTS

The government should establish a duty for public and private organisations to publish accountability documents such as ROPAs, DPIAs, LIAs and International Data Transfers Assessments, in recognition of the key role these instruments have in ensuring transparency, accountability and public trust over data uses.

Accountability requirements such as DPIAs, ROPAs) LIAs and International Data Transfers Risk Assessments are not only legal duties, but important tools to identify risks of data processing upfront, and prevent harms from occurring in practice. The pivotal importance of these documents was also acknowledged by the former Information Commissioner in her "lessons learnt" report that followed the Covid-19 crisis.[203]

However, in each of the Covid-19 programmes analysed in this report, a DPIA was noticeably absent (or not public) at the beginning of the programme. Matt Hancock's response to these failures, that the government should not bother with bureaucracy,[204] reveals how these were not isolated mistakes, but the outcomes of poor data and risk governance. In turn, these politically motivated actions led to the occurrence of material harms, such as Test and Trace data being shared on social media and misused to harass women. Failure to place data protection principles front and centre also led to delays in the roll-out of important public health measures such as the NHS Covid-19 App.

TRANSFER RESPONSIBILITY FOR APPOINTING THE INFORMATION COMMISSIONER FROM GOVERNMENT TO PARLIAMENT

The prerogative power to appoint the Information Commissioner, oversee their function, and to allocate the budget for the ICO, should be transferred to Parliament, as recommended by Parliament in 2003,[205] 2006,[206] and 2014[207]

This change would strengthen the independence of the ICO. The Covid-19 case-studies of this report revealed a concerning attitude from the Information Commissioner, who seemed more concerned about "acting as a critical friend" and managing their relationship with the Government rather than fulfilling their statutory duties and bringing public programmes in line with legal requirements.

The DPDI Bill aims to formalise the government power to interfere with the independent functioning of the Commissioner, as well as to introduce secondary statutory objectives that would undermine the objectivity of the ICO and the clarity of its mandate. Instead, the UK data protection reform should focus on increasing arms-length between the government and the ICO.

---

203 https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf

204 https://twitter.com/OpenRightsGroup/status/1285260608875700225

205 https://publications.parliament.uk/pa/cm200203/cmselect/cmpubadm/165/165.pdf

206 https://publications.parliament.uk/pa/cm200506/cmselect/cmconst/991/99109.htm#a22%2044

207 https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/11009.htm

CLARIFY THE ICO'S PRIMARY RESPONSIBILITY

The Government should clarify the statutory objective of the ICO, specifying that it has a principal duty to fully enforce information rights laws with all due diligence.

The Schrems II judgment, which constitutes retained EU case law, already clarified that the principal objective of supervisory authorities is to "monitor the application of the GDPR and to ensure its enforcement", as well as to handle complaints "with all due diligence" and in light of anyfindings "to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence".[208] The UK adherence to this judgment is also a centrepiece of the UK Adequacy Decision, which ensures the free flow of data to and from the EU.[209]

Transposing these duties into primary legislation would put the full and diligent enforcement of information rights front and centre to the Commissioner's mandate.

IMPLEMENT ARTICLE 80(2) OF THE UK GDPR, AND ALLOW PUBLIC INTEREST ORGANISATIONS TO BRING OPT-OUT REPRESENTATIVE ACTIONS

New data protection legislation should implement Article 80(2) to allow public interest organisations to litigate against data abuses without the constraint of obtaining the authorisation of each affected individual. This would encourage the filing of well-argued, strategically important cases with the potential to significantly improve the data protection rights of individuals as a whole.

Actionable data protection rights, such as the right to lodge a complaint, are important mechanisms to ensure public scrutiny and a key fail safe in the event of oversight failures. This was proven during the pandemic: while the ICO faded into the background and failed to keep the Government in check, civil society and the public were able to step in to and challenge the Government's illegal conduct.

REFORM SECTIONS 165 AND 166 OF THE DATA PROTECTION ACT 2018 TO ALLOW THE INFORMATION TRIBUNAL TO ORDER THE USE OF THE COMMISSIONER'S ENFORCEMENT POWERS

New legislation should amend Sections 165 and 166 of the Data Protection Act 2018 so that there is oversight through the Information Rights Tribunal of the appropriateness of the ICO's action in response to complaints on both substantive and procedural grounds. This should include the power for the tribunal to order the ICO to rely on their enforcement powers and take remedial action.

208 https://curia.europa.eu/juris/document/documentjsf;jsessionid=3212DE51C069861DA306DB63306D0DE7?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3435549

209 https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf

5.2 RECOMMENDATIONS FOR THE ICO

AUDIT GOVERNMENT DEPARTMENTS TO ENSURE PROPER DATA GOVERNANCE

The ICO should ensure that government departments have a thorough understanding of proper data governance, starting with an audit of key government departments' use of DPIAs and the quality of their Data Protection Officers. This preventative and forward-looking approach to public sector enforcement would ensure that sound data governance structures are adopted before a time of crisis.

UTILISE STRONGER ENFORCEMENT MECHANISMS

The ICO should move away from its over-reliance on reprimands, and move toward a more assertive use of enforcement and penalty notices instead. This would ensure that legal requirements are implemented within a defined time-scale, and that government departments can be held to account if they fail to comply with these notices.

DEVELOP CONCRETE SYSTEMS FOR OVERSIGHT DURING EMERGENCY SITUATIONS

The ICO was unprepared to deal with the myriad challenges posed by the COVID-19 pandemic. While some difficulties adjusting to an unprecedented situation are understandable, the organisation has yet to demonstrate that new safeguards and protocols are in place to ensure it can continue to function effectively during challenging circumstances in the future. The ICO plays a key role in the oversight of the government's handling of data so it is vital that it is completely independent from government.

Using the blueprints laid out by other DPAs and UK regulatory bodies like the FCA, the ICO needs to create emergency protocols that will enable it to maintain strong oversight and the ability to respond quickly during emergency situations.

BETTER INCORPORATE THE PUBLIC INTO THE ICO'S WORK

The ICO's remit is to uphold information rights in the public interest. To better achieve this aim, the regulator should run public consultations or deliberative exercises annually to ensure the Commissioner understands and can prioritise public expectations and areas of concern for information rights. By involving the public more thoroughly, the ICO can better promote public trust in the systems designed to ensure proper government and business use of data.

6 CONCLUSION

The Covid-19 pandemic prompted the use of novel and wide-reaching technology as part of a public health response. The unprecedented generation, storage, and analysis of public health data revealed the cracks in the UK's data protection regime. An analysis of three uses of public health data revealed clear holes in the programmes' transparency and accountability: excessive retention of data, missing and late DPIAs, and the involvement of private companies without proper safeguards. Amidst this crisis for public health data, the ICO was largely absent, unwilling to take strong enforcement action, or late to the game.

To improve the strength of data protection standards and future responses to emergency situations, the ICO must move away from its 'critical friend' approach and use of non-binding reprimands and take stronger enforcement action against companies and the government when they breach data protections. The ICO must also implement protocols for emergency situations that will allow the regulator to respond quickly and provide thorough oversight. Additionally, the government must drop its DPDI Bill – the bill presents a clear threat to the UK's data protection framework and would further exacerbate the many issues identified with data protection for public health data during the pandemic.

As the UK government pushes forward with a £480 million contract for the Federated Data Platform, which is strongly tipped to be won by Palantir – a global firm that has expressed little regard for public accountability and data protection[210] – there is significant risk that the UK public could find itself with fewer rights, and a regulator unable to enforce them. A new approach is needed, one that utilises the lessons learned from the pandemic to ensure a clear and comprehensive data protection framework in the UK that protects individuals' fundamental rights.

210 https://www.amnestyusa.org/wp-content/uploads/2020/09/Amnest-International-Palantir-Briefing-Report-092520_Final.pdf

openrightsgroup.org