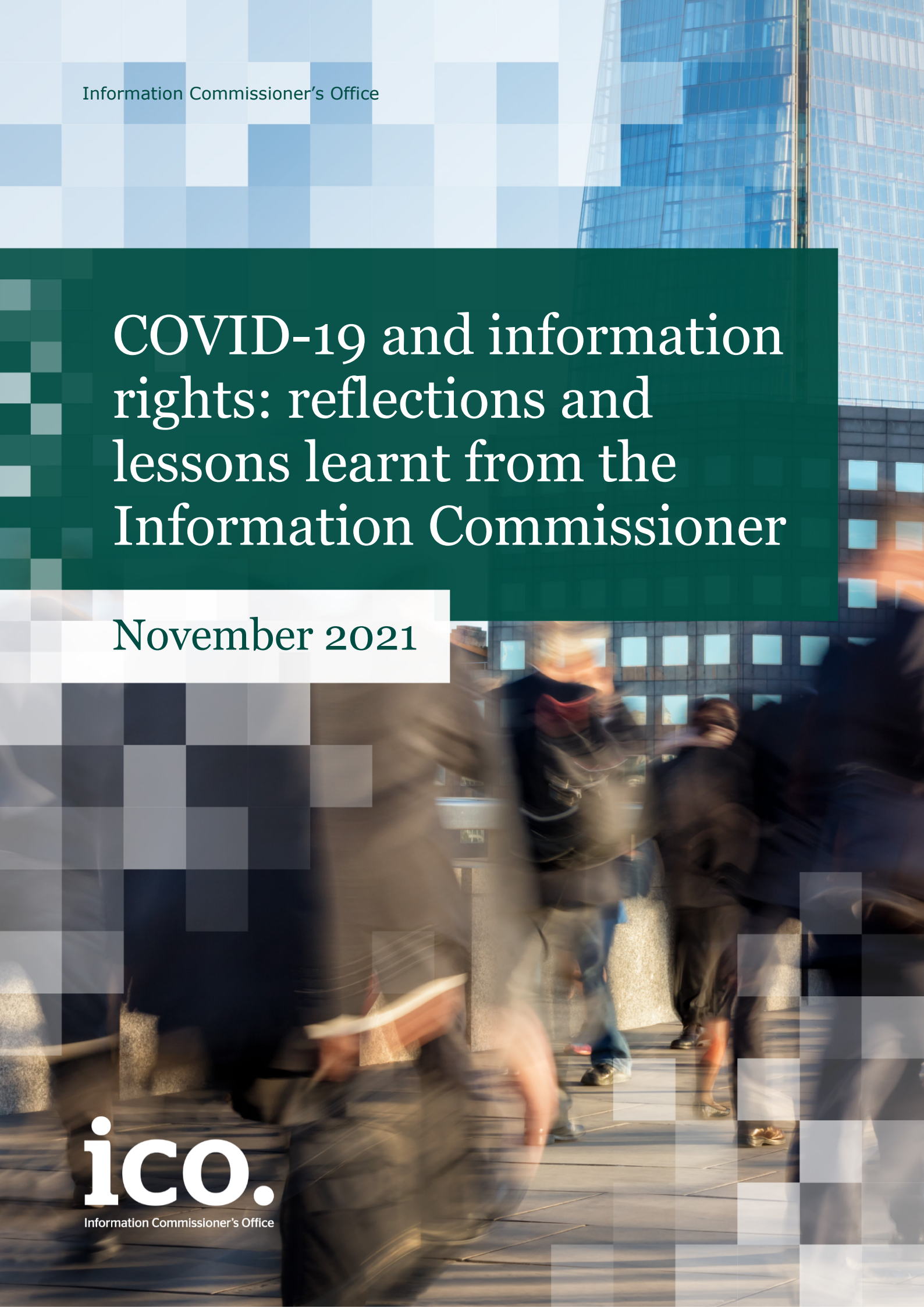
Information Commissioner's Office

COVID-19 and information rights: reflections and lessons learnt from the Information Commissioner

November 2021



ico.
Information Commissioner's Office

Contents

Introduction

On 11 March 2020, the World Health Organisation declared the outbreak of COVID-19 a pandemic. From that point on, governments and societies across the world were faced with a range of unprecedented challenges. The measures that were taken to tackle them would change our lives profoundly. In some cases, these measures will impact how citizens and societies interact and operate for years to come.

Governments asked their citizens to accept restrictions on their freedoms not seen before in peacetime. To protect public health, the UK Government, like those of other democracies, had to balance competing rights. For example, the rights of freedom of movement and assembly being restricted, to protect the right to life.

Most citizens accepted and understood these restrictions as necessary to protect themselves, their families, and their communities. But restrictions came at a significant cost to many people's physical, emotional, and financial health. Broader decisions on public spending, for example, will have an impact on society for generations to come.

The obligation on governments and public bodies to account for these decisions and make available the information behind them couldn't be greater. From the outset of the pandemic the ICO put transparency at the heart of our approach to regulating access to information. Whilst at the same time, we recognised the challenges being faced by public authorities, who needed to focus resources on delivering essential services to vulnerable citizens.

The COVID-19 pandemic is the biggest global public health crisis in over a century. But thanks to the transformational power of science, data and technologies it was possible to develop responses at pace. Fuelling the functioning of these technologies was citizens' personal data. On a local and national level, data collection, analysis, and sharing were pivotal to fast, efficient, and effective delivery of pandemic responses, particularly for the most vulnerable in society. Be it through the shielding programme or national contact tracing systems.

At the outset of the pandemic, I believed that two issues would be central to the successful delivery of digital and technological solutions. The first was whether the flexibility of the data protection legislative framework and system of regulation would enable the innovative use of data and still provide protection to individuals. The second was ensuring that citizens would have sufficient trust in the way their data was being used by organisations responsible for developing these solutions to guarantee public engagement and support.

These are two of the issues I explore in this short policy paper. I reflect on some of the key themes and emerging issues in information rights regulation that my

office has grappled with over the last 18 months. The paper also considers the impact these developments might have on the domestic and international information rights landscape and regulating in the public interest.

Few aspects of life have been untouched by the pandemic. The efforts to combat it have drawn on the resources and intelligence of all sectors of society. As the Information Commissioner, I have had the privilege of playing a part in supporting these efforts. As we continue our recovery for the pandemic, my office continues to advise and support governments and organisations across the UK. This is to ensure that data can be used to deliver innovative, needs-driven public services that have the trust and confidence of the public.

At the time of writing, most restrictions on our day-to-day lives in the UK have been lifted, but the effects of the pandemic continue to be felt both here and around the world. As my term of office as the UK's Information Commissioner comes to an end, it remains as clear as ever to me that privacy protections and transparency of decision-making are parts of modern life that we must not lose, however difficult the circumstances.

I hope this paper, alongside the evidence I have provided to Parliament[1] during the pandemic on my office's approach, will contribute to the public debate and record.

Elizabeth Denham CBE
November 2021

[1] Joint Committee on Human Rights
The Government's response to Covid-19: human rights implications
Elizabeth Denham
Monday 4 May 2020

Select Committee on Public Services
Public services: lessons from coronavirus
Elizabeth Denham & Steve Wood
Wednesday 22 July 2020

Data protection legislation and the response to the pandemic

In early 2020, when it became clear that the world was facing a health emergency like no other, governments began to ask whether:

- existing legal frameworks would be sufficient to deal with the challenges of managing a global pandemic in the modern era; and
- any additional emergency legislation would be necessary.

For data protection, the question being asked both in the UK and across the western world was whether existing legal frameworks would be:

- flexible enough to allow for the collection, sharing and use of personal data in the delivery of vital services; and
- not present legal barriers to the use of tech innovation to respond to the challenges of COVID-19.

As the UK regulator for information rights, I make two broad observations. The first is that the principles-based approach of the law had the flexibility we needed, when we needed it. As the regulator, I was able to apply a pragmatic risk-based approach to overcome any challenges within the legislative framework. We didn't need to change the law to allow for nationwide test and trace systems, or to allow for the data sharing that was necessary to support the vulnerable. These key principles also provided 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.

This doesn't mean we didn't encounter challenges in interpreting the complexity of the law, when providing the necessary regulatory assurance and support to organisations developing key responses. The interpretation of the principle of "necessity" in the use of temperature testing by businesses and organisations, required some complex thinking. But none of these issues were insurmountable and the law therefore worked as it was intended to.

My second observation is that where the law works best – or perhaps where organisations best understood the law - was where people's privacy expectations were considered front and centre through the development of digitally-enabled responses and projects. This was a time for privacy protection by design – in practice.

I was clear from the outset that my office would have an important role to play in those projects. Both by enabling progress that can help society and by protecting the people whose data, and trust, such projects relied on. This was set out in my regulatory approach published in April 2020[2]. At the heart of this was how we would put into practice the ex-ante and ex-poste or end-to-end

[2] How we will regulate during coronavirus | ICO

regulation responsibilities data protection law provides me. This was integral to the effective regulation of a whole range of COVID-19 responses, proximity apps, customer logs and test and trace programmes.

Our engagement with the England and Wales NHS COVID-19 App and their counterparts in Scotland and Northern Ireland is a good example of the ex-ante approach we took.

We engaged in discussions about data protection and contact tracing apps from the start. We published a formal Opinion about the joint Google – Apple exposure notification API[3] and then developing a detailed expectations document[4], which served as a reference point throughout.

We did not have a seat at the design table, but we were consulted by the governments from the outset and provided advice on a privacy by design and default approach. Our role was to ask questions on how transparency, legality and fairness would be built-in to the project and prompt the right considerations to be made.

This also resulted in a valuable assessment of the protections for data when using decentralised mobile device level applications against centralised systems. Whilst I was clear that this was not a binary, good-bad discussion, the benefits that a decentralised approach offer for data minimisation were significant and as a driver public trust. There were also welcome contributions to these discussions from academics and civil society.

Central to this was the Data Protection Impact Assessment (DPIA). DPIAs are sometimes viewed as bureaucratic 'tick box' exercises that hinder rather than encourage innovation. But engaged early as a central tool in the design process, organisations can identify potential risks and mitigate those during the development stage (and lifecycle of the product). – This is how they were treated by the Department of Health and Social Care and the Devolved Administrations, This risk and mitigation process benefitted both the business or organisation and individuals and consumers.

In this element of the pandemic response, DHSC and the Devolved Administrations provided iterations of the DPIAs and responded constructively to feedback. This prompted changes, including:

- improved privacy information;
- how individuals could exercise their rights;
- greater security of data; and
- clearer information about the use of automated decision-making.

[3] Apple and Google joint initiative on COVID-19 contact tracing technology (ico.org.uk)
[4] https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf

Active engagement on DPIAs during the pandemic all yielded positive results both for individual privacy and trust and engagement in the schemes themselves. For example, customer logs and the supermarkets' vulnerable persons data-sharing scheme.

Working with an organisation as it develops its programme does not remove our ability to take formal action if necessary (ex-poste actions). And our regulatory role does not end once an innovation is launched. Our future engagement on the NHS COVID-19 app will focus on the data protection implications of any changes to the app's functionality.

When I appeared before the Joint Committee on Human Rights last year about the COVID-19 app, members expressed concern about the compatibility of our ex-ante and ex-poste roles. In particular, our appetite to take enforcement action against an organisation when we have previously provided data protection advice during the design and development process of a product or service. I recognise that theoretical concern. But the nature of regulating in the digital era, where potentially intrusive technologies are being used that could impact on individuals rights, means that it is not responsible for the regulator to only intervene once the product has been developed. Being involved from the outset is a vital part of our role as an enabler and protector. I have also ensured that the ICO has the governance and decision-making processes to ensure the effectiveness of both regulatory elements.

We have also recently completed an audit of the processing of personal data for administering the DHSC's NHS Test and Trace Programme (T&T). The audit recognises that the T&T Programme was established and is operating within the context of responding to a public health emergency. But also that it has now moved into the established framework of English health protection arrangements. This more long-term arrangement was considered whilst conducting the audit. I am reassured that UK Health Security Agency (UKHSA) has accepted all my recommendations to strengthen the governance of this, the largest, public data collection arrangement in many years. The recommendations contain significant and important actions that I expect UKHSA to implement swiftly. I will continue to monitor their progress in response to our audit.

It is of course right that we reflect whether there are lessons to be learnt from the pandemic. I therefore welcome the government's consultation "Data: A New Direction" as an opportunity to review the UK data protection framework and regulatory regime. The consultation makes several proposals that aim to provide greater clarity in the law for businesses and organisations. For example, the processing of data in a health emergency.

One of the proposals is to remove the requirement to conduct DPIAs. This would be replaced by a more general requirement to have assessed and appropriately mitigated the risks arising from data processing. I agree that there is scope for more flexibility about the form assessments take. But, as I have previously set

out, DPIAs were essential in the success of the Privacy by Design approach taken to the development of digital solutions during the pandemic and enabled the twin objectives of public health and individuals privacy rights to be met.

I therefore welcome recognition by the Government of the value of an independent ICO. An independent regulator assures the public of their protections and maintains trust in data-driven innovation. For the future ICO to be able to hold government to account, it is vital its governance model preserves its independence and is workable, within the context of the framework set by Parliament and with effective accountability. The current proposals for the Secretary of State to approve ICO guidance and to appoint the CEO do not sufficiently safeguard this independence. I urge the Government to reconsider these proposals to ensure the independence of the regulator is preserved. My office is actively engaging with government on these law reform proposals and our detailed response to the consultation can be found at Response to DCMS consultation "Data: a new direction" (ico.org.uk).

Impact of the pandemic on transparency and accountability

The other part of my remit as Information Commissioner is freedom of information and transparency. The Freedom of Information Act (FOIA) provides the public with a right to know about the activities of public authorities, unless there is a good reason not to. It is now an important foundational right in most western democracies.

We recognised that many public authorities subject to FOIA were also the organisations at the frontline of delivering services to the public and vulnerable citizens during the acute stages of the pandemic. Many had less capacity than normal, and resources normally dedicated to information rights work were diverted elsewhere. At the same time, staff often had limited access to buildings due to national and local lockdowns.

An impact on timeliness in responding to information requests was therefore inevitable. We took account of this when processing requests and enforcing disclosures to ensure the impact was proportionate at a time of national crisis. However, it is worth noting that the impact was less than might have been expected for central government. Government Departments responded to 87% of requests they received on time in 2020, compared to 93% in 2019[5]. This demonstrates that despite the pressures of the pandemic, organisations continued to take their access to information duties seriously.

As a regulator, my focus during the pandemic therefore was on transparency and encouraging public authorities to proactively publish information on issues that they knew would be important to their communities. In particular, key decisions and public spending. I also placed an emphasis on good record keeping so that decisions could be subject to public scrutiny in the future.

I therefore welcomed innovations at a local and national level to proactively put information on the pandemic response into the public domain:

- the UK Government's daily briefings that provided real-time information about the course of the pandemic;
- accompanying data sets that were made available on gov.uk; and
- the daily statistics released by the four UK nations on cases, hospitalisations, deaths, and vaccination rates.

All of this helped to inform public understanding about the impact of the pandemic across the UK.

But there are examples of where COVID-19 pressures have impacted on proactive disclosure. Most notably, a National Audit Office report "Investigations into government procurement during the COVID-19 pandemic" last year. It

[5] Freedom of Information statistics: annual 2020 - GOV.UK (www.gov.uk)

found a lack of transparency and inadequate documentation of some key decisions in the early part of the pandemic in procurement and contracts. The NAO recognised these were exceptional circumstances. However, they said it remained essential that decisions about how tax-payers money is spent is properly documented to maintain public trust. Proactive disclosure of public sector procurement contracts is something I raised in my 2019 "Outsourcing Oversight report"[6]. I believe the pandemic provides a further trigger to support re-examination of these recommendations.

I would also highlight the recent FOI decision notice my office issued to the Department for Health and Social Care[7], ordering them to disclose the names of 47 companies which were awarded contracts via the "high-priority lane" for procuring PPE.

The pandemic has also brought to the fore the importance of good public record-keeping. During the last 20 months, governments have made decisions about public health, public spending and civil liberties. Many of the effects of these decisions will be with us for years to come. It is through transparency that people can understand why these decisions were made and trust them. And it is through documenting these decisions that lessons can be learned for the future and, in time, inform the historical record. Having a record of decisions for others to access in the future is also essential to good administration.

I was concerned when reports emerged that Ministers and senior officials used private email and messaging channels to conduct sensitive official business during the pandemic. The use of private communications channels for official business does not in itself break freedom of information law. But without clear processes in place, information contained in these channels can be forgotten, overlooked, auto-deleted or otherwise not available when a freedom of information request is later made. This frustrates the freedom of information process and puts at risk the preservation of official records of decision-making.

There is also a concern that the use of private email channels will place security of personal data at risk, if any emails contain such information. My concern would grow if this also included more sensitive information related to members of the public. I will therefore also focus on the data protection risks of the practice.

That is why my office launched a formal investigation into the use of private correspondence channels at the DHSC in July 2021. That investigation will establish if private correspondence channels have been used, the extent of use, and if their specific use led to breaches of freedom of information or data

[6] outsourcing oversight (ico.org.uk)
[7] ic-94513-n5h8.pdf (ico.org.uk)

protection law. We will publish the results of that investigation in due course, and it would therefore not be appropriate for me to comment further here.

Separately, I note that there are several ongoing judicial reviews about the reported use of private email accounts by government Ministers on issues relating to the pandemic, including the awarding of contracts. One of the areas under challenge is whether the current policy on the use of private email channels is fit for purpose in ensuring accountability and transparency in government decision-making. I also note the evidence that has been recently disclosed to the Courts on use of private email as part of these claims.

The practice of using private communications channels to conduct parliamentary and government business is not a new issue for my office. The ICO, successive governments and The National Archives have previously emphasised the important principle of transparency around government decision-making. The Government's own S46 records management code of practice also sets clear standards and emphasises the importance of good records management in ensuring public trust and confidence, particularly following a national crisis. The National Archives operates its Information Management Assessment Programme; and my office has recently updated guidance on official information held in private communication channels that reflects the practical realities of some of our ways of working[8]. We will continue to remind public authorities of the importance of good records management and supporting them to get this right.

The Government's commitment to hold a public inquiry into its handling of the coronavirus pandemic next year is welcome. It represents an important step in demonstrating transparency and accountability in decision-making by governments and public bodies during this unprecedented period.

It also presents an opportunity to have a debate about the meaning of a public record and public record keeping in the digital era. When FOIA came into force in 2005, the internet and emails were still relatively new office tools and smartphone messaging apps didn't exist. The workings of government and public authorities were still largely paper-based and what constituted a public record was more clearly understood. Since then, the volume and range of communication mediums has grown exponentially and are now increasingly used by Ministers and officials in public bodies to communicate on a range of issues. In some cases, the messages generated could constitute a public record but might not be recognised as such at the time and are therefore not treated as one.

This debate could also provide the opportunity to look at the case for a new and stronger legal "duty to document" to be placed on Ministers, public servants and others who are responsible for maintaining the public record. This is not a novel

[8] Official information held in non-corporate communications channels | ICO

idea. Similar duties already exist in Canada, New Zealand and the USA. A duty to document does not need to be onerous. The focus is not on the creation of more records, but rather on the creation and retention of the right records and the documents to be created will depend on the mandate and individual public authorities. We also need to continue to examine whether the right systems, training, governance, and support are in place for digital records management. This is ultimately a risk that must be owned and managed by senior public officials and ministers. In an era of fast-paced digital decision-making I believe this is a necessary step to ensure continued accountability, trust, and transparency in our democracy.

International collaboration during the pandemic

The response to the pandemic, by definition, required international cooperation. This was particularly the case in the use of personal data which flows quickly and easily across borders and is central to the governments' co-ordination of public health action.

As chair of the Global Privacy Assembly (GPA), my office was able to act quickly in April 2020 when we chaired the first GPA-OECD forum. This brought together data protection authorities, government, academics and Google and Apple to look at the data governance and privacy challenges in tackling COVID-19. A common theme during this early discussion was international comparisons of approaches to contact tracing and particularly protecting privacy through the use of apps and biometrics.

The pandemic also highlighted the value of the international instruments that contain common global principles, such as the Council of Europe Convention 108 and the OECD privacy guidelines. They enabled a global language and a common approach to maintaining high standards of trust and transparency in the context of COVID-19.

A follow-up GPA-OECD workshop was held in September 2021 by which point many countries were entering the containment and recovery stages of the pandemic. We examined the continuing development of digital technologies and data sharing arrangements. This included those that can track the spread of the virus and assist research efforts to develop a vaccine. What was clear from our discussions with other data protection authorities was that the most successful solutions in terms of public trust were those that engaged the advice of the data protection authority early. This ensured best practice on data protection and privacy was at the heart of the design model.

International collaboration can also support the promotion of good practice and consistent approaches. A good example of this was the GPA Executive Committee's joint statement on the sharing of health data for domestic and international travel purposes published in March 2021. It outlined the principles of effectiveness, necessity and proportionality that must guide the development of COVID-19 certification or passports. A common global approach is essential in international travel to ensure public trust and confidence. The GPA was also able to share this statement with the WHO and OECD, to inform and support the standards they are developing for international travel mobility.

In terms of transparency, as Chair of the International Conference of Information Commissioners (ICIC), I co-signed a resolution with many of my colleagues at the start of pandemic highlighting "the value of clear and transparent communication, and of good record-keeping, in what will be a much-

analysed period of history"[9]. Our work on the ICIC has helped us deliver the objectives I set out in the ICO's access to information strategy "Openness by Design"[10] to develop and sustain our international partnerships. The resolution was also reflected in my office's regulatory approach domestically and again demonstrates that countries across the world are grappling with similar issues in the digital era.

I am very proud of what the information rights international community achieved during the pandemic. I hope both the GPA and the ICIC continue to provide leadership and influence as the world continues its recovery from COVID-19.

[9] International Conference of Information Commissioners website
[10] Openness by design (ico.org.uk)

COVID 19: Challenges for the recovery and beyond

Earlier in the paper I set out some of the learnings from regulating data protection and access to information during the pandemic. In particular, the importance of end-to-end regulation in building trust and confidence in innovative products and technologies – essential in a public health emergency. This approach recognises the importance of early advice and consultation, linked to data protection by design principles. But also, an expectation by the public of ongoing monitoring and assessment of how solutions protect personal data in practice. The use of audit powers and ultimately enforcement powers must remain part of a full process of regulation.

Going forward, data protection must play a continuing and sustained role in the recovery from the pandemic. There will be lessons we can learn from the experience of the COVID-19 apps. These will feed into the development of ongoing solutions, including the use of vaccination certification both for travel and in a domestic setting, where the importance of privacy preserving systems will remain. This means:

- decentralising as much of the operation as possible;
- minimising data exposure for checking and certification; and
- recognising that data requirements can differ for international travel and domestic uses (the latter requiring less data).

Another area that will continue to need scrutiny is the role of third parties in the ecosystem of health data in the future and their responsibilities to the data being processed. Third party contractors have played a key role in the delivery of a number of pandemic responses. This includes the Test and Trace system, where most public facing roles are delivered by third parties. Third parties are also offering AI and biometric services to health bodies. It is therefore essential that the governance arrangements:

- build-in sufficient oversight of the processing being carried out by third parties, including DPIAs being in place; and
- ensure there is due diligence around transparency and effective purpose limitation safeguards are in place.

Looking further ahead, there will rightly be challenging questions on how long these systems should be in place and to avoid a creep towards disproportionate long-term health surveillance. There will be the inevitable demands to use COVID-19 data sets for new purposes and research. Part of the role of the regulator is to ensure applications are effectively shut down when no longer needed and sunset clauses and review periods are respected or effectively actioned. It will also be the role of government, parliament, and civil society to debate the measures and data collection that continue beyond the emergency. We will also assess the benefits of using Trusted Research Environments. This

will provide a Privacy by Design approach that allows targeted access to anonymised and pseudonymised datasets, to ensure transparency of use, particularly where sensitive personal data is involved.

Data protection regulators will continue to play an important role in providing end-to-end regulation during the recovery period and beyond.

Conclusion

In my introduction I raised two issues that were salient at the outset of the pandemic:

- whether the flexibility in the law allowed data protection to be both an enabler of innovative data use and yet still provide protection to individuals; and
- how public confidence in the use of that data could be maintained.

In my view, the flexibility built into the law, based upon proportionality, has meant that we have been able to support innovative uses of data to counter the pandemic. But also that the tests of fairness, reasonableness and transparency built-in to the law have helped to maintain public trust in that data use. The existence of an independent regulator to oversee these protections has proved vital – ensuring that privacy has been central to the design process. My conclusion is that high standards of data protection have been shown to help rather than hinder the use of data for public good.