Explanatory Framework for Adequacy Discussions

Section B: Wider Context

Overview

This section sets out the UK's wider digital and technological landscape and the UK Government's initiatives in that space. It explains how aspects not directly related to data protection – such as building a resilient cyber-infrastructure or championing human rights – indirectly underpin the UK's data protection framework and are essential for its effective functioning.

Section B: Wider Context

Introduction

Over the last few decades, data has become an ever more important element of modern life. Whether personal, transactional, sensor, web, or "big data", various forms of data now permeate every aspect of citizens' daily lives and shape their everyday interactions.

Data underpins public services and can be considered 'critical infrastructure', not just for delivering those services today, but for the advanced technologies of tomorrow. This will deliver better services more efficiently. As a forward-looking government, we believe it is imperative to shape the wider landscape that enables the continuous growth and use of data.

Data is also a key component in the fight against crime. The proportionate use of data helps the police to protect the public by catching criminals and tackling organised cross border crime. It assists the police to apprehend suspects, the Crown Prosecution Service in bringing cases to court, and the courts in delivering effective justice.

Government-driven initiatives, such as our proposals for a new regulatory framework for online harms, or the establishment of institutions exploring artificial intelligence (AI), together create a thriving data ecosystem in which citizens feel encouraged to participate, while remaining confident that their data is treated to the highest standards.

The UK Government is strongly committed to protecting the personal data of citizens and will continue to be a global leader in ensuring such data remains safe. This commitment rests on a holistic approach to data. Legal provisions governing the protection of personal data alone do not result in high data protection standards. A comprehensive set of measures is needed alongside, designed to create a digital environment in which individuals can feel assured that their data won't be compromised.

These "building blocks" of the digital space, from resilient physical infrastructures to independent data advisory boards, are the key to **maintaining trust and confidence in the use of personal data**. It is for this reason, the UK's data protection framework and the landscape within which it sits remain a priority for the UK.

This document sets out the various aspects that shape the UK's digital environment and, ultimately, underpin the UK's strong data protection framework.[1]

Human Rights

[1] The ICO's various codes of conduct as well as initiatives in the law enforcement or national security space e.g. the establishment of the Biometrics Commissioner, are covered in their respective sections of this pack rather than in this section.

Section B: Wider Context

All of the UK Government's efforts are underpinned by a strong commitment to protecting and respecting human rights. The UK has a longstanding tradition of ensuring rights and liberties are protected domestically and of fulfilling international human rights obligations.

The UK has strong human rights protections within a comprehensive and well-established constitutional and legal system, and the decision to leave the EU does not change this. Human rights are protected through, for example, the Human Rights Act 1998 and the devolution statutes. The Human Rights Act 1998 gives further effect in UK law to the rights and freedoms contained in the ECHR. This means that any person in the UK can enforce their ECHR rights in a UK court or tribunal.

Individuals can rely on their human rights in the UK courts and seek remedy for any infringement. Under the Human Rights Act 1998, if a court finds that a public authority has acted in a way that is incompatible with a Convention right, it can award any remedy within its powers that it considers to be just and appropriate. This may include, for example, damages. If the individual is unsuccessful in the domestic courts (including through any available appeal rights), he or she can take their case to the European Court of Human Rights.

The UK is a founding member of the Council of Europe and was one of the first countries to ratify the European Convention on Human Rights. The Council of Europe and the ECHR have a leading role in the promotion and protection of human rights, democracy, and the rule of law in wider Europe. The UK is committed to membership of the ECHR, and will continue to be a party to the ECHR after it has left the EU.

The UK's record at the European Court of Human Rights further demonstrates the UK's commitment to ensuring human rights are protected. The UK has the lowest number of applications per 1 million inhabitants of all Member States.[2] At the end of 2018, cases against the UK made up only 0.2% of the Court's ongoing caseload.[3]

The Future of the UK's Digital Environment

Digital Charter

Alongside the new opportunities the digital age offers, there will be new challenges and risks. Citizens rightly want to know that they will be safe and secure online. Tackling these challenges in an effective and responsible way is critical for digital technology to thrive.

The Digital Charter is the UK's answer: it aims to ensure digital innovation is supported whilst simultaneously protecting the personal data, rights and interests of citizens. The Digital Charter's core purpose is to make the internet work for everyone – for citizens, businesses

[2] 5.34 applications per 1 million inhabitants. Germany has 5.9 applications, Ireland 6.2 and Denmark 6.4.
[3] For context, the UK constitutes 8.0% of the population of all Council of Europe Member States.

and society as a whole. The internet is a global network and the UK will work with other countries that share both the UK's values and determination to get this right.

The Digital Charter is an iterative programme of work. It is guided by the following set of principles:

- the internet should be free, open and accessible;
- people should understand the rules that apply to them when they are online;
- personal data should be respected and used appropriately;
- protections should be in place to help keep people safe online, especially children;
- the same rights that people have offline must be protected online;
- the social and economic benefits brought by new technologies should be fairly shared.

The Digital Charter has an ambitious work programme, spanning across various areas of the digital ecosystem. These will be explored in more detail throughout this document. Up to date, the UK Government has:

- published a Social Media Code of Practice, which sets expectations for preventing and responding to abusive behaviour, and annual transparency requirements;
- taken a range of actions to raise cyber security standards across the UK, backed by £1.9bn of new funding, including the creation of the National Cyber Security Centre;
- published a Code of Practice for Internet of Things devices to ensure that strong security is built into internet-connected products by design;
- set new standards for protecting personal data, and through the Data Protection Act, has given people more rights and control over the use of their data;
- established the Centre for Data Ethics and Innovation - an advisory body which provides the UK government with independent, expert advice on the measures needed to enable and ensure safe, ethical and innovative uses of AI and data-driven technologies;[4]
- published the independent Cairncross Review, which considers how the news industry in the UK can become more sustainable as it transitions from print to digital;
- published an independent review of competition in the digital economy, undertaken by an expert panel in digital competition led by Professor Jason Furman;
- through the Intellectual Property Office, facilitated a Code of Practice signed by search engines and copyright owners, which has reduced the prominence of websites hosting illegal copyright infringing content in natural search results.

Among other things, the UK Government will:

[4] This is set out further below.

- introduce a new statutory duty of care, which will be overseen and enforced by an independent regulator, as set out in the Online Harms White Paper.[5] This regulatory framework will require companies to take reasonable and proportionate action to tackle harmful online content and activity on their services;
- engage with the Centre for Data Ethics and Innovation to examine areas that pose key policy challenges;
- assess how online advertising is regulated in the UK, recognising the need to fully consider the different challenges brought by online advertising to develop an effective response;
- continue to develop a National Data Strategy to unlock the power of data across government and the economy, while building public trust and confidence in its use;
- set out our response to the range of challenges posed by digital markets as part of wider work to update the UK's competition regime.

Technology is always evolving and so will the Charter, adapting to respond to new challenges and opportunities. To do so in a holistic way, the UK Government will look to the tech sector, businesses and civil society to own these challenges and find solutions together.

Priorities for the UK Government include protecting people from harmful content and behaviour through the Online Harms White Paper, ensuring data is used in a safe and ethical way, looking at the legal liability that social media companies have for the content shared on their sites, limiting the spread of disinformation and making sure that companies have suitable cyber security.

Cybersecurity

A secure environment is the foundation of a functioning society and a strong data protection framework. The UK is committed to protecting its citizens and their data online, and has a highly effective regime to help prevent cyber attacks and data breaches. Cyber threats are treated as a 'tier one' risk in the National Security Strategy, alongside terrorism, international military conflict and major natural hazards.

To ensure that the UK is a safe place to live and do business online, the National Cyber Security Strategy (2016–21) sets out ambitious policies to protect the UK in cyberspace, backed with £1.9 billion investment. The vision is for the UK to continue being secure and resilient to cyber threats, prosperous and confident in the digital world.[6]

In 2016, the National Cyber Security Centre (NCSC) was opened to further that goal. The NCSC is a unique centre of cyber security expertise which protects the public and draws

[5] This is outlined further below.

[6] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

upon the world-leading capabilities of GCHQ: part of an intelligence agency but with a specific new public-facing role which includes protecting citizens online.

In June 2018 it conducted a public consultation,[7] pitching its own role to ensure those who govern and regulate the use of data across sectors do so effectively. The NCSC operates by drawing on evidence and insights from across regulators, academia, the public, and business. It then translates these into recommendations and actions that deliver direct, real-world impact on the way that data-driven technologies and AI are used. **In its first two years, the NCSC has defended the UK from 1,167 major cyber attacks**.

NCSC programmes such as the *Active Cyber Defence* (ACD) programme provides greater protection for the public and NCSC expertise is being used across government to help secure online public services and the data they hold. **ACD has reduced the UK's share of visible global phishing attacks by more than half (54%) - from 5.3% to 2.4%.** Between September 2017 and August 2018, the service removed 138,398 UK-hosted phishing websites attempting to obtain personal data. Since its inception, the programme has had a significant impact in tackling the vast amount of malicious websites and phishing emails which seek to steal citizens' personal data.

Another important initiative is the UK Government's approach to *Secure by Design*, the first genuine national attempt to address cyber security issues around the rapid proliferation of internet-connected devices. In 2018, the UK Government published the first ever *Code of Practice* to encourage device manufacturers and software developers to ensure their products are *secure by design*, with security built in from the start.

Another key document is the new *Guidance for Consumers, a simple guide* which shows citizens how to protect their smart devices and their personal data. The UK recognises the importance of cybersecurity in safeguarding citizen's privacy and is working to internationalise the UK's approach and encourage other nations to help develop common standards to improve device security and protect personal data.

Online Harms

In April 2019 the Government published its Online Harms White Paper, which sets out its plans for a world-leading package of online safety measures that also supports innovation and a thriving digital economy.

As outlined in the White Paper, the Government intends to establish in law a new duty of care on companies towards their users, overseen by an independent regulator. Companies will be accountable for tackling a comprehensive set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal. The duty of

[7] https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation#ministerial-foreword

care will ensure companies have appropriate systems and processes in place to deal with harmful content on their services, and keep their users safe, especially children and other disproportionately affected groups.

The new regulatory framework will increase the responsibility of online services without interfering with the current limitations of liability for platforms. The UK believes systemic improvements in platforms' risk management and processes will be more effective in preventing harm than a focus on liability.

Moreover, the White Paper commits the UK Government to a variety of non-legislative measures. These include a national online media literacy strategy, which will ensure a coordinated and strategic approach to online media literacy education and awareness for children, young people and adults. The White Paper also includes a commitment to producing a safety-by-design framework, offering guidance, especially for start-ups and small businesses, about how to embed safety during the development or update of products and services.

As a responsible and democratic Government, a full 12 week public consultation was conducted on the government's plans for regulation and tackling online harms, which elicited over 2,300 responses. In February 2020, the Government published its Initial Consultation Response to the Online Harms White Paper. It set out a detailed summary of the consultation findings, the extensive engagement we have conducted since publishing the White Paper, our direction of travel on a number of key areas, and our intended next steps.

We believe our approach can lead towards new, global approaches for online safety that support our democratic values, and promote a free, open and secure internet; and we will work with other countries to build an international consensus behind it. The UK, along with other like minded democracies, actively promotes the multi-stakeholder approach to Internet governance.

National Data Strategy

The UK Government is developing an ambitious programme to ensure the UK remains at the forefront of the international modernisation agenda, that it maintains the UK's global top 3 position in the development of Artificial Intelligence (AI) technologies, and provides credible, global leadership in the positive and ethical use of data and technology.

The National Data Strategy (NDS) aims to unlock the power of data in the UK economy and government, while building public confidence in its use. It will help ensure that people, businesses and organisations trust the data ecosystem, are sufficiently skilled to operate effectively within it, and can get access to high-quality data when they need it.

Section B: Wider Context

The NDS will provide coherence and impetus to the wide range of data-led work across government while creating a shared understanding across the economy of how data is used. It will bring together the UK's data strengths and opportunities within a single, government-wide narrative, driving the collective vision that will support the UK to build a world leading data economy.

A two-phase consultation process and call for evidence were announced at London Tech Week on 11 June 2019, with work with the public and across government conducted in Autumn 2019 to define its 2030 Vision. Fuller stakeholder engagement and consultation is planned prior to launching the UK Government's National Data Strategy in 2020.

In the UK Government's first call for evidence, a provisional set of objectives were highlighted that were divided into 3 areas of focus:

People

1. To ensure that data is used in a way that people can trust.
2. To ensure that everyone can effectively participate in an increasingly data-driven society.

Economy

3. To ensure that all businesses and non-profit organisations can effectively operate in an increasingly data-driven economy.
4. To improve growth and productivity through the effective use of data across the economy.

Government

5. To improve public services and government operations through the effective collection, sharing and use of data.
6. To achieve alignment in government around data, with data shared and used cooperatively wherever appropriate.

The National Data Strategy will cover both personal and non-personal data.

Data Policy and Governance

The UK Government relies on access to data to carry out its many functions, which range from developing evidence-based policy to delivering world class public services. The UK is working to establish cross-government approaches to data that support good data stewardship and and secure access to data where it is appropriate.

The UK has established the Data Advisory Board and the Data Leaders Network to provide cross-government leadership on data and drive change through Data Enabled-Change Accelerator (DECA) projects. The UK has also introduced new data sharing powers within

Section B: Wider Context

Part 5 of the Digital Economy Act 2017 to provide greater legal clarity around the specific purposes for which specified public authorities can disclose and process personal data. The powers are designed to improve the sharing of publicly held information for the following specific purposes:

Public service delivery	Allows for data sharing to support services and (positive) interventions for citizens and households as part of social and economic policies. Examples include supporting individuals and households with multiple disadvantages (e.g. Troubled Families) and/or living in fuel/water poverty.
Civil registration	Enables flexible sharing of civil registration information (births, marriages and deaths). Civil registration data can play a big part in supporting digital transformation that benefits the individual. e.g. checking against birth record data can confirm eligibility for a service without the need to send paper copies.
Debt	Allows organisations to quickly establish data sharing pilots to test the value of data sharing to reduce and manage debt owed to government.
Fraud	Provides the ability to quickly establish data sharing pilots to test data-enabled methods to combat fraud.
Research	Permits public authorities to share de-identified information with accredited researchers for the purposes of research in the public interest
Disclosure by Revenue Authorities	Enables Her Majesty's Revenue and Customs, the Welsh Revenue Authority and Revenue Scotland to share general and aggregate data to allow them to play a wider role in policy development.
Statistics	Supports the reuse of administrative data and access to real time data to produce up-to-date national and official statistics.

The UK Government is championing the powers, such as the public service delivery power, and is working with a range of stakeholders, as well as the wider public sector to support the uptake of these powers. We are also working to improve the discoverability of data within government and have established a cross-government group to consider what should be captured in departmental data inventories and how they should be maintained. The UK Government is also looking at data quality and what can be done at a cross-governmental level to better understand and improve the quality of our data.

Section B: Wider Context

Cross-government work on improving access to data also extends to users outside the public sector. The UK is a world leader on open data and is ranked joint first with Canada in the World Wide Web Foundation's Open Data Barometer[8]. The UK Government releases open data on a range of topics and we continue to drive challenging commitments to ensure that the UK continues to innovate and lead on this important agenda.

HMG Framework for Data Processing

The UK Government takes both the protection of personal data and the right to privacy extremely seriously. In the execution of the UK Government's functions is an inherent requirement to process significant volumes of personal data. The UK Government recognises the strong public interest in understanding better how they process that data. The Framework is intended to set out the principles and processes that the UK Government should have regard to when processing personal data. It does not give the UK Government any new powers to share or process data, but will further improve the transparency and clarity of existing government processing.

Centre for Data Ethics and Innovation

The UK Government set up the Centre for Data Ethics and Innovation (the 'CDEI') to provide independent, expert advice on the measures needed to enable and ensure safe, ethical and innovative uses of AI and data-driven technologies.

The CDEI published a report on Online Targeting in February 2020, and will publish papers on Data Sharing in the Public Sector and Facial Recognition Technology.

- The CDEI recommended that platforms should be required to maintain online advertising archives, including of political adverts, to provide transparency for types of personalised advertising that pose particular societal risks, and to help ensure that elections are not only fair but are seen to be fair.
- The CDEI also recommended that the online harms regulator is given the power to require online platforms to give independent researchers secure access to their data. The Government will respond to the CDEI's recommendations within 6 months.
- The CDEI has released snapshot papers on 'Deep Fakes', 'AI and personal insurance' and 'Smart speakers'. They are planning to publish papers on facial recognition technology and data sharing in the public sector in the coming weeks, as well as the AI Barometer, which considered the key risks and opportunities of AI in 5 key sectors. In addition, they will publish their report on algorithmic bias in March 2020.

The Centre identifies the measures needed to strengthen and improve the way data and AI are used and regulated. This includes promoting best practice and advising on how we address potential gaps in our regulatory landscape. The CDEI was set up to ensure that data and AI-driven innovations continue to deliver maximum benefits for society, whilst also

[8] https://opendatabarometer.org/?_year=2017&indicator=ODB

driving the highest standards for transparency and accountability when building or buying new data technology. It operates by drawing on evidence and insights from across regulators, academia, the public and business, then translates these into actions that deliver direct, real world impact on the way that data and AI is used.

The UK already benefits from a world-class regulatory regime, and the CDEI will build on this by making sure we understand and respond to the rapidly evolving way in which data impacts our lives.

The CDEI published its first Work Programme and Strategy in March 2019 setting out its priorities and ways of working. The 2019/20 Work Programme sets out the CDEI's focus in its first year of operation. This includes reviews on bias in algorithms and online targeting.

AI and Data

AI covers a set of complementary, general purpose, technologies that build on current digital applications to automate more complex actions than have been automated before, offering enormous improvements in reliability, efficiency, and productivity.

In the Autumn 2017 Budget, the UK Government announced funding for a set of AI institutions to address the Grand Challenge: an 'Office for AI' to coordinate work in AI across government; and an industry/academia-led AI Council, to work with the Office for AI by advising on how best to address the Grand Challenge.

A priority area of work for the Office for AI is exploring mechanisms to facilitate legal, fair, ethical and safe data sharing that is scalable and portable to stimulate AI technology innovation. This reflects the recommendations of the AI review, which have been firmly committed to in the Industrial Strategy of the AI Sector Deal. This included a partnership with the Open Data Institute in 2019 on two 'Data Trusts' pilots, tackling illegal wildlife trade and food waste[9]. Other priority areas of work include improving the skills pipeline for AI and data-driven technology careers,[10] and encouraging adoption across the economy.

In driving AI adoption across the economy, the Office for AI is exploring a variety of incentives to focus efforts on addressing a particular aspect of the Grand Challenge on AI and Data.

In May 2018, the previous Prime Minister announced a mission to use AI and Data to transform the prevention, early diagnosis and treatment of diseases such as cancer, diabetes, heart disease, and dementia by 2030. This will require new ways of working with

[9] https://theodi.org/article/odi-data-trusts-report/

[10] https://www.gov.uk/government/news/next-generation-of-artificial-intelligence-talent-to-be-trained-at-uk-universities

individuals' health data that simultaneously affords strong data protection whilst allowing health data (with appropriate consent) to be used safely and ethically to drive forward medical research and improve people's lives.

National Data Guardian for Health and Social Care

New technologies and ways of sharing data mean that we can now gain huge benefit from the sharing of health and care data, both in terms of individuals' own care and the broader social good of advancing research and treatment. However, this cannot come at the expense of privacy.

The National Data Guardian (NDG) for Health and Social Care, sponsored by the Department of Health and Social Care, operates independently, with the aim of building trust in the use of data across health and social care.[11] The Health and Social Care (National Data Guardian) Act 2018 placed the role of the NDG on a statutory footing.

The Act gives the NDG the power to publish formal guidance, and provide informal advice, assistance, and information to anyone, about the processing of health and adult social care data in England. It also imposes a corresponding duty on public bodies and providers within the health and adult social care sector to have regard to the formal published guidance.

Placing the NDG on a statutory footing has been significant in strengthening this independent, authoritative voice for the patient and service user on how their data is used in the health and adult social care system.

ePrivacy/Privacy and Electronic Communications

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) implemented the E-Privacy Directive (2002/58/EC). They were introduced in recognition of the growth of digital mobile networks and the internet, which opened up new possibilities for businesses and users, but also new risks to their privacy. The PECR complement the United Kingdom General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018 and specify more detailed privacy rights for electronic communications.[12]

The PECR have strengthened the UK's law in areas including direct marketing, use of cookies, security of public electronic communications services, and the privacy of customers using communications networks or services with regard to traffic and location data, itemised billing, line identification services, and directory listings.

[11] https://www.gov.uk/government/speeches/national-data-building-trust-across-health-and-social-care.

[12] The UK has also retained the substantive requirements of EU Regulation 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (with appropriate amendments).

Section B: Wider Context

The UK Government has taken a number of actions to reduce the number of nuisance calls, which are a particular concern to people in the UK. This has included a ban on cold calls from personal injury firms and pension providers, unless the consumer has explicitly agreed to be contacted; the introduction of director liability for nuisance calls; funding of a call blocking project initiative for vulnerable people; and the introduction of Calling Line Identification (CLI) when calls are made for direct marketing purposes.

The Information Commissioner's Office (ICO) is the independent supervisory authority responsible for enforcement of PECR. It can impose fines of up to £500,000 for breaches of PECR. It also engages closely with other regulators, such as the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA), on investigations of shared interest.

Privacy and Consumer Advisory Group

As shown throughout this document, the UK Government is undertaking a variety of initiatives with implications for individuals regarding the use of their personal data and their privacy.

The success, credibility and viability of such programmes depend upon their trustworthiness. The UK Government requires independent review, analysis, guidance and feedback on these initiatives from organisations and individuals with expertise in the areas of privacy and consumer interests. To achieve this, the Privacy and Consumer Advisory Group (PCAG) has been established.

PCAG is a forum that:

- provides an independent view on issues involving privacy and wider consumer concerns;
- brings together a broad range of expertise in privacy and consumer issues to engage with the UK Government in an open and mutually-respectful environment where issues can be discussed candidly and honestly;
- ensures that the UK Government programmes engage effectively to incorporate issues related to citizen privacy, trust and confidence during each of the design phases – from initial policy planning to requirement specification through to delivery, with the aim of improving the eventual design and implementation of the programmes;
- provides a channel for the UK Government and wider public sector engagement with representatives from the privacy and consumer sectors;
- advocates and promotes privacy-friendly approaches to the handling of personal information;
- clearly communicates and explains privacy and consumer issues; and
- develops and agrees PCAG's key messaging, and monitors the UK Government's developments and the extent to which expert input is implemented.

PCAG aims to ensure:

- users are in control of their information;
- information isn't centralised; and
- users have a choice of who provides services on their behalf

They do this by providing independent review, analysis, guidance and feedback on government identity assurance and data-related initiatives.[13]

All of this demonstrates the UK's commitment to protect personal data and uphold the rights of citizens whilst making the best use of the available technology.

Surveillance Camera Commissioner

The UK's commitment to a high standard of data protection is further evidenced by the existence of the Protection of Freedoms Act 2012, which led to the creation of the Surveillance Camera Commissioner. The Act requires that a code of practice about surveillance camera systems has to be produced, including guidelines for CCTV and automatic number plate recognition.

The role of the Surveillance Camera Commissioner is to encourage compliance to the code of practice, to review how it is working, and to provide advice to ministers on whether the code needs amending. Furthermore, the Surveillance Camera Commissioner submits an annual report to the Home Secretary, which is then laid before parliament. This report outlines the work which the Commissioner has done and their plans for the future.

The Surveillance Camera Commissioner has no enforcement or inspection powers, rather they work with relevant authorities to make them aware of their duty to regard the code.

Upholding the principles of necessity and proportionality within the DPA 2018, the code sets out the balance between upholding civil liberties and protecting the public through its twelve guiding principles.

Section F contains further information on the Surveillance Camera Commissioner.

[13] Minutes from the group's meetings are available at: https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group.