techUK
FOR WHAT COMES NEXT

Trust, innovation, and global leadership:

getting data governance right in the UK in 2021

March 2021

Contents

Executive summary and recommendations for action 06

Introduction 12

1. Supporting and encouraging data-driven innovation 16

2. Increasing trust through a meaningful and proportionate approach to data protection 24

3. Becoming a leader in the global debate on data 30

In 2021, the UK is facing a new era in its history.

A future outside the European Single Market and Customs Union, as well as facing the challenge of rebuilding its economy after the COVID-19 pandemic. While we cannot fully predict the changes which will come in this new era, what is certain is that the increased adoption and use of digital technologies seen in 2020 is set to continue.

Unlocking the full benefits of these technologies is vital to our economic future. However, the UK's ability to realise the full economic and social potential of advanced data-driven digital technologies will only be achieved if there is also trust and confidence in the development and use of these innovations.

Right now, there are many questions being asked about which direction the UK will take in 2021. The UK Government's National Data Strategy published in December 2020 sent a strong signal for the UK's next steps. The Strategy is driven by five missions: **unlocking the value of data across the economy**; **maintaining a pro-growth and trusted data regime**; **transforming the Government's use of data**; **ensuring resilience and security in data infrastructure**; and **championing international flows of data**.

Striking the right balance between trust and innovation is crucial to achieving the aims outlined in the Strategy and maximise the opportunities of data and technology to improve our lives.

However, this will not happen on its own. We must take action to position the UK as a pioneer in developing a living data protection system. Once able to embrace and encourage a greater synergy between privacy and innovation, the UK will be able to guide, steer and influence the global debate about the future direction of data governance and privacy in a way which protects the global digital economy and guards against the fragmentation of the internet.

Achieving this requires a detailed conversation about getting data governance right for what comes next in an ever-changing world.

techUK has developed this discussion paper to encourage and aid this debate. It includes suggestions of key areas where transformation is possible to help the UK position itself as a world leader in achieving a data governance system underpinned by solid principles, a clear and consistent approach and able to flex and evolve to maintain trust and confidence even as new technologies emerge.

Executive summary and recommendations for action

1. Supporting and encouraging data-driven innovation

Create new ways and approaches to support innovators, by building a living and adaptable data protection regime

> DCMS should create a Data Governance Forum, built on and driven by regular engagement and consultation between industry and government, to create the space for collaborative discussion on issues raised by emerging and transformative technologies.

> Expand the use of sandboxes with a focus on creating sandbox schemes across all sectors and regulators.

> The UK should become a leader in demonstrating and supporting how privacy regulation can enable digital innovation through the revised Industrial Strategy, and the R&D Roadmap.

Removing existing barriers to innovation

- Consideration should now be given to finding new, agreed pathways to widen the use of government held personal and non-personal data by the private sector, for example in the health sector, and how increased regulatory coordination, between the Information Commissioner's Office (ICO) and regulators such as the Health Research Agency (HRA) could be encouraged to find innovative ways data could be used to develop new services.
- Organisations looking to use advanced analytical cookies, to support and enable data-driven innovation, should benefit from legislative clarity and certainty.

Embed innovation in a more systemic approach to data protection and privacy across government and regulators

- A strategic forward-looking review is needed of all current, and future planned, government initiatives and projects to better understand how data privacy issues are being raised and discussed, who is involved, whether innovation is being encouraged, and to what extent there is coordination between departments and engagement with the ICO.
- Coordination between regulators is crucial to avoid overlap and contradictory decisions. A similar assessment should be taken for regulators working in this area including what can be learnt from the new regulator's forum created by ICO, the Competition and Markets Authority (CMA) and Ofcom.
- Establish regular feedback loops to allow common problems or issues around the interpretation or application of data protection rules to be identified and policies to be updated where appropriate.
- Ensure key stakeholders including civil society experts are able to engage in the process through regular consultations, reviews or periodic public dialogues.

2. Increasing trust through a meaningful and proportionate approach to data protection

Bringing clarity and certainty to existing rules

> Engage with industry to develop guidance which provides more legal clarity and certainty on increasingly complex, difficult, and burdensome areas of the current legal framework, such as an overreliance on consent as a legal basis. The UK should review where the ICO could be even more effective as a regulator to support, guide, oversee, and enable meaningful compliance with data protection laws, utilising the different legal bases in the GDPR.

> Develop an international data transfer regime that provides tools for global data transfers. The regime should support compatibility with our closest partners such as the EU, but also provide pathways for managed data transfers across the globe, including practical steps to improve UK transfer regime, such as increasing the speed of Binding Corporate Rules (BCRs) approval and establishing the UK's transfer tools on a strong legal footing.

Making the paperwork of privacy more meaningful

> Government should conduct an analysis of the current administrative requirements under the wider UK data governance legal framework including UK GDPR and Privacy and Electronic Communications Regulations (PECR) to assess where the paperwork being required is providing meaningful support to the objectives of UK data protection laws and identify where current administrative requirements could be reformed or streamlined to help businesses focus their resources.

> This assessment should also identify how cutting-edge technologies including blockchain, AI and automation, could help to meet our objectives to protect privacy.

Having a regulator that provides certainty and supports compliance

> Government should ensure the ICO is effectively supported to underpin a data governance system that balances trust and innovation

3. Becoming a leader in the global debate on data

Credibility

- The UK must be alive to different tensions that exist between data protection regimes around the world and work with allies to establish bridges and prevent the fragmentation of approaches to data protection and data transfers.
- However, we must lead by example and develop a data governance system that promotes trust while also enabling innovation.
- We will also need to walk the walk as well as talk the talk by being robust in our efforts to prevent regulatory isolation, in areas such as data localisation at home as well as abroad.

Openness

- Create a variety of pathways for data transfers, looking to countries like Japan and New Zealand and how they have blended a mix of free trade agreements and transfer tools to create a variety of options for firms.
- The UK needs a dual track approach, continuing to recognise the use of EU data transfer tools, while also creating new UK SCCs, BCRs and codes of conduct to give companies a suite of transfer tools.
- The UK should also use its trade agenda to export these values of ensuring there are legal methods to transfer personal information across borders.

Leveraging our alliances

> Create new pathways for data transfers through trusted and easy-to-understand data transfer tools.

> Leverage our alliances to engage at multilateral level to promote common principals, tools and data protection practices which lay the groundwork for new pathways for global data to flow.

> Seize the opportunity to become an active and thoughtful participant in the global debate on data so that firms interested in seeking to shape and influence global rules see the UK as a potential base for research and thought leadership.

Introduction

In 2021, many are watching what the UK will do now as it begins its future outside of the EU Single Market and Customs Union. The publication last year of the Government's National Data Strategy offered insights into the vision and strategy that is now being explored on how the UK can unlock the full value and power of data. The consultative approach and engagement with industry on how the National Data Strategy can be taken forward has been welcomed by industry. However, techUK believes that the UK can, and should, go further and take action now to get data governance right for the UK's data-driven future.

Having a modern, agile, pioneering, forward-looking, adaptable, innovation-supporting, and privacy-first approach to data governance will allow the UK to become a beacon to global innovators looking to develop cutting edge technologies that can be trusted and deployed globally.

This means developing a regulatory system and put in place structures for data protection that are clear, consistent, and meaningful. As well as a legal, regulatory and policy environment that can flex and evolve.

This will be a key competitive advantage to the UK as its looks to its future outside of the EU.

It will send a clear message that the UK approach to data privacy goes beyond regulation and compliance. It is about having a living, evolving, responsive data protection system that can adapt, remain relevant and meaningful to people's everyday lives. Greater trust and confidence in the system and structures that underpin data innovation will be key to driving adoption, take up and use of the next wave of innovative digital products and services.

Positioning the UK as a pioneer in how to embrace and encourage a greater synergy between privacy and innovation will send a powerful message to other regions and countries around the world looking to do the same.

This paper outlines action that can be taken in the following three areas to achieve this world leading system and approach:

1. **Supporting and encouraging data-driven innovation**
2. **Increasing trust through a meaningful and proportionate approach to data protection**
3. **Becoming a leader in the global debate on data**

Before outlining in more detail the areas where action can be taken to achieve this opportunity, it is important not to overlook the context within which this discussion is taking place.

Importance of UK GDPR to where we are today

In May 2018, the UK implemented the EU General Data Protection Regulation (GDPR) into UK law. The introduction of the GDPR provided a clear, common, principle based, technology neutral regulatory and legislative framework. The UK GDPR has empowered UK individuals, for example, by introducing a specific right to request deletion in certain circumstances directly from the data controller, and the right to correct inaccurate data directly with the data controller instead of through the courts. The introduction of the GDPR also introduced the first industry-wide data breach notification requirement and enhanced data security requirements by imposing security obligations on data processors as well as data controllers. The GDPR has also been key in underpinning the UK's work on digital and data ethics.

While the GDPR is not an ethical framework, it has provided the legal foundations and basis on which organisations have been able to develop and operationalise ethical codes and guidelines.

However, the GDPR is not infallible and must be read in conjunction with the evolution of EU law which has made significant interpretations of the GDPR since 2018. Data protection must be an evolving practice and, now that we have left the EU, and are no longer subject to its courts, the Government should look at how we evolve the UK GDPR in a way that suits the UK's interests.

Current context - The importance of securing Data Adequacy

On 28 December 2020, the UK and EU agreed on a new Trade and Cooperation Agreement (TCA) which set the new terms of trade for business from 1 January 2021. Alongside the UK-EU TCA the UK and EU published a statement allowing a further, up to six-month, bridge period to allow for the completion of a UK adequacy decision.

The UK was deemed by the European Commission to be adequate on 19 February 2021. This must now be approved by the European Council.

However, adequacy is not a permanent status; the Commission's decision will be scrutinised, must be renewed at least every four years, and there is the underlying possibility of UK adequacy being challenged in the courts. Therefore, as the UK and EU data protection systems evolve independently of one another, both the UK and the EU have a strong incentive to ensure they maintain compatible high standards that support the continuation of the free flow of personal data.

1. Supporting and encouraging data-driven innovation

By supporting innovation, the UK can lead in the development and commercialisation of new products, services and solutions that can enhance individual's data privacy, meet the fundamental objectives of data protection, and build greater trust and confidence in data-driven digital technologies. To achieve this, we must:

- Create new ways and approaches to support innovators, by building a living and adaptable data protection regime
- Remove existing barriers to innovation in the current data protection regime; and
- Embed innovation in a more systemic, joined up, coordinated approach to data protection across government and regulators.

Create new ways and approaches to support innovators, by building a living and adaptable data protection regime:

The evolution of technologies such as AI, IoT will raise new data protection and privacy questions that will need to be identified and addressed. Digital innovators developing the next generation of cutting-edge data-driven technologies want to get data protection right.

However, to ensure data protection and privacy do not become a barrier to the development of future digital technologies in the UK it is suggested that DCMS create a Data Governance Forum, built on and driven by regular engagement and consultation between industry, government and civil society, where innovators could alert government to possible data governance issues, raised by emerging and transformative technologies.

The UK should look to create an environment that supports innovators to better understand and address data protection and privacy issues and concerns that could be raised in the development of emerging technologies. The development and running of a sandbox by the ICO is an effective example of how the UK has already demonstrated global leadership in taking a new, modern approach to helping to raise understanding of data governance issues and support innovators.

Sandboxes are highly effective tools, allowing regulators to engage with the market, while also supporting innovators to test out new products in a secure environment and with oversight. This synergy helps drive better regulatory outcomes and ensures that regulators are aware of the leading technologies and innovative practices in their sector. The use of sandboxes should therefore be scaled up, expanded and applied across all sectors and regulators. The sandbox system should provide as much flexibility to innovators as possible to ensure the benefits of data-driven technologies are realised while maintaining security and protection of data to suitable levels.

The UK should also look to identify ways to stimulate and support the development of new innovative technologies that can help to protect individual's data and enable privacy. The UK should become a leader in demonstrating how privacy can be an enabler, rather than a barrier, to digital innovation. For example, by supporting the development of next generation of Privacy Enhancing Technologies (PETs) through the Industrial Strategy Challenge Fund and the work to take forward the R&D Roadmap. The recent RUSI Future FIS project[1] that brought together industry, government leaders and regulators to consider how PETs could be applied to address practical data sharing problems that currently exist is an example of how innovation can be supported.

Removing existing barriers to innovation:

For technological innovation to flourish in the UK, it is important that any existing barriers to the development of cutting-edge innovation that exist today are unlocked. Particularly where these relate to existing data protection and privacy laws.

The following are three examples of areas:

> **Medical and health innovation**

> **Digital Identity**

> **Development and use of advanced data analytics**

[1] https://www.future-fis.com/

Medical and health innovation

The UK already has a unique capability in relation to health data. The UK also has a well-developed data governance regime for health data research with initiatives such as the Clinical Practice Research Datalink, a real-world research service supporting retrospective and prospective public health and clinical studies, having been in place for thirty years. The work of the Nuffield Council on Bioethics is another an example of where the UK has an international reputation on issues around health and innovation. The UK is also seen as leading in the development and use of AI within healthcare. The goal now should be for the UK to position itself as the world leader in not just research but the development of cutting-edge health innovation.

During COVID-19 government recognised the use of existing derogations within UK GDPR to allow the use of health data in the public interest. NHSX have set up the Centre for Improving Data Collaboration to support the health sector in establishing data sharing partnerships with industry. Their aim is to create an environment that allows the NHS and patients to realise the benefits of cutting-edge research and tech. Additionally, they exist to provide a voice for industry in discussions shaping the UK's innovation landscape.

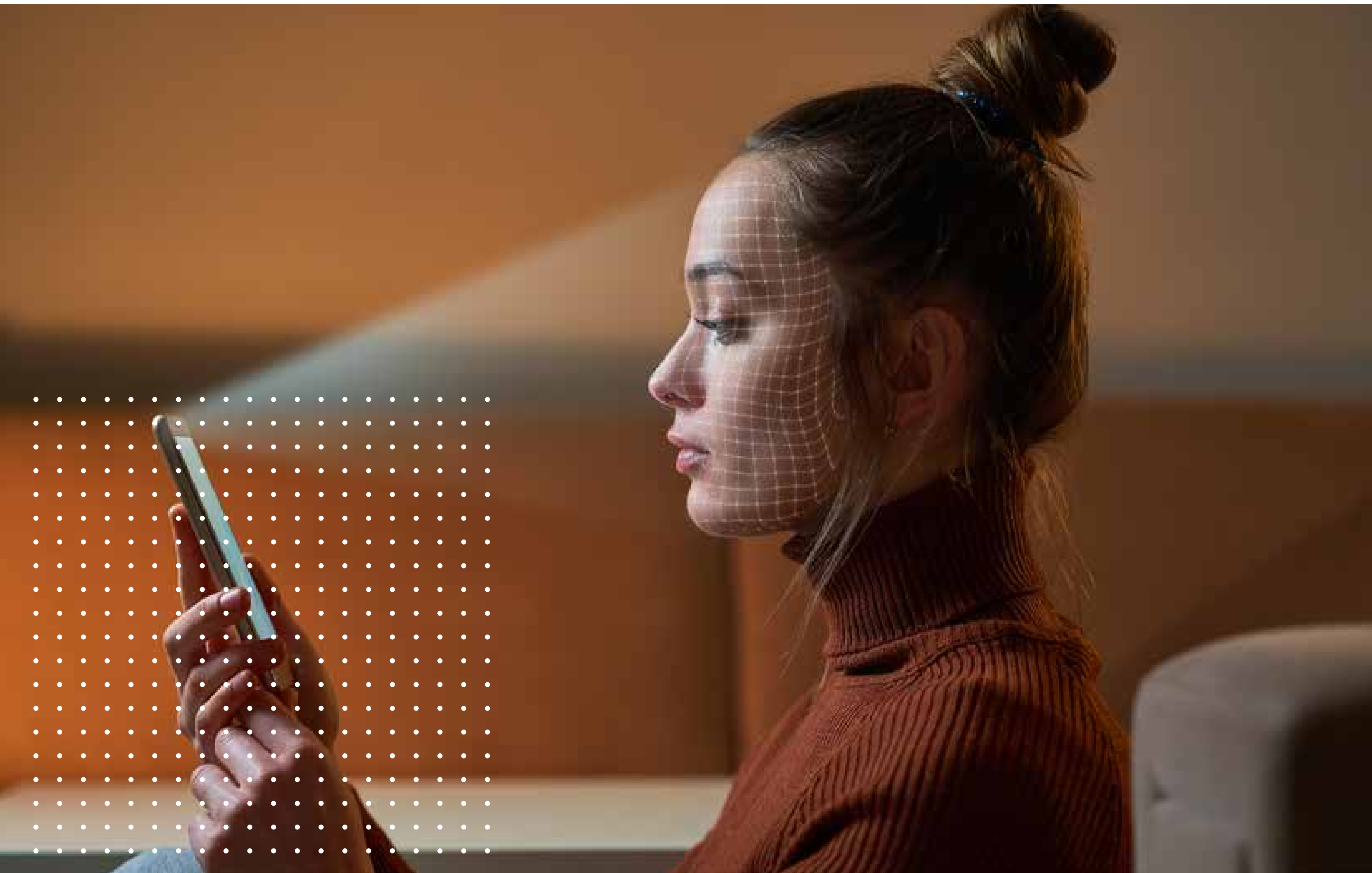
Consideration should now be given to whether there may be additional ways to open wider the use of health data. For example, it is suggested that the government could examine the effects of derogations used during the pandemic and consult with the public, NHS and industry to assess whether further derogations could help improve health outcomes. Moreover, how could more regulatory coordination, for example between the ICO and the HRA, be encouraged to find innovative ways health data could be used?

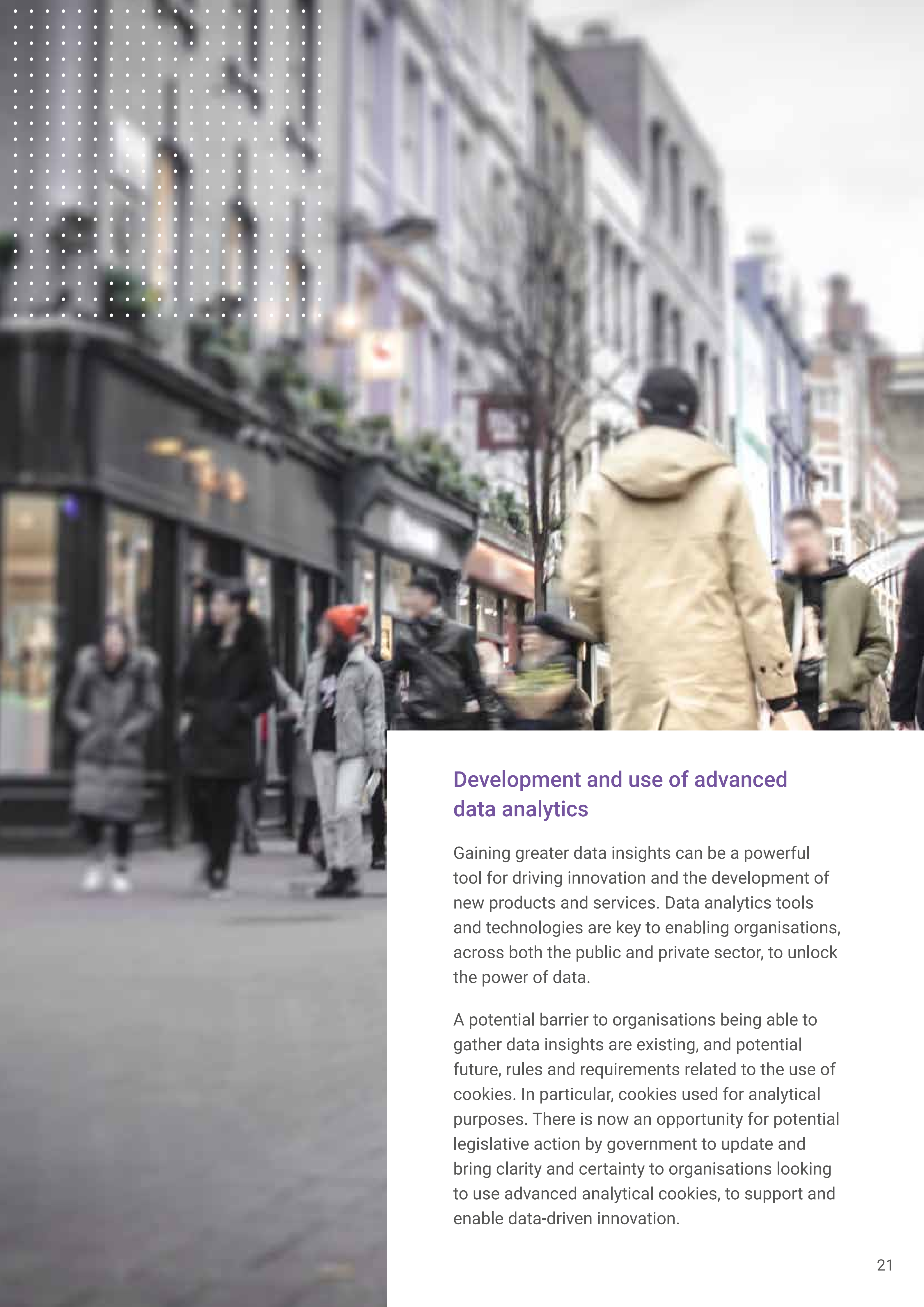
Digital Identity

Managed properly, Digital ID and strong authentication can provide security for data and can be an enabler of better data governance. Now that the exchange of data has become fundamental to a large part of economic activity, it is essential that data be kept secure and that data subjects can be clearly identifiable where required (e.g. subject access requests under the Data Protection Act). When combined with multifactor identification such as device ID and biometrics, digital IDs become a secure method of verifying one's identity. Digital identity can also support greater data minimisation by reducing the need for physical copies of identity documents to be transferred and stored.

Digital ID is an example of innovation that could support and enable greater data privacy and a solution that will be meaningful and impactful to individuals in their everyday lives.

Using a digital identity, citizens could access a digital ecosystem, which pulls data from numerous sources, thereby allowing innovative uses of this combined data, increasing efficiencies and obviating multiple log-ins. In addition, digital identities offer greater security, enhance data-privacy and customer control while also combatting fraud and identity theft. The UK could become a global leader in the development and adoption of Digital ID. For this to happen, Government action is needed to remove current barriers to the development of a Digital ID in the UK. For example, access to a number of Government databases (e.g. passport and driving licences) via API for verified Digital ID companies to help confirm an individual's identity is needed. A new lawful basis for processing biometric data for identity verification and authentication purposes should also be introduced.





Development and use of advanced data analytics

Gaining greater data insights can be a powerful tool for driving innovation and the development of new products and services. Data analytics tools and technologies are key to enabling organisations, across both the public and private sector, to unlock the power of data.

A potential barrier to organisations being able to gather data insights are existing, and potential future, rules and requirements related to the use of cookies. In particular, cookies used for analytical purposes. There is now an opportunity for potential legislative action by government to update and bring clarity and certainty to organisations looking to use advanced analytical cookies, to support and enable data-driven innovation.

Embed innovation in a more systemic approach to data protection and privacy across government and regulators:

Data protection and privacy issues are increasingly raised and discussed across all industries and sectors. Equally, within Government, different department's data strategies and initiatives are raising data privacy related issues. For example, the Department for Business, Energy and Industrial Strategy (BEIS) Smart Data Review and the Department of Transport Future of Mobility strategy. Industry often faces the same questions about data governance from different departments and regulators including the ICO, the Financial Conduct Authority (FCA), Ofcom and bodies such as the National Data Guardian.

Given the number of separate, and sometimes uncoordinated, overlapping and duplicated, discussions around data privacy it is becoming increasingly difficult for organisations, particularly innovators, to understand the direction the UK is headed in, what is being required and how they can engage and input. As a result, innovators may not be able to develop common tools and solutions that can be offered and easily deployed by multiple government departments or bodies. There is a real concern that a continued lack of consistency in the strategic vision and approach being taken to data will result in the development of inconsistent policies, procedures and requirements that will also become an ongoing barrier to innovation.

These multiple data protection discussions rarely consider the role innovation could play in overcoming privacy-related issues or the challenges being faced. The role of innovation is often seen as an afterthought with the focus squarely on applicable laws, rules, and legal compliance. This is a missed opportunity to encourage the development of innovative solutions to common issues being faced across government and regulated sectors.

There's a clear opportunity for the UK to be a global leader in building a more systemic approach that will increase coordination in Government and between Regulators on data issues. This, in turn, will put innovation at the heart of government's data policies and initiatives.

Any systematic approach should be based on clear principles, seek to involve key stakeholders and be underpinned by transparency so that civil society, Government, the industry and experts are able to engage in the process. This could be facilitated through regular consultations, reviews or periodic public dialogues. Developing such a systematic approach will be vital for achieving that prized balance between trust and innovation.

A review and assessment is needed of all current, and future planned, government initiatives and projects to better understand how data privacy issues are being raised and discussed, who is involved, whether innovation is being encouraged, and to what extent there is coordination between departments and engagement with the ICO.
A similar assessment should be taken for Regulators working in this area including what can be learnt from the new Regulators forum created by ICO, CMA and Ofcom.

The goal should be to find a new joined up approach where departments and regulators are able to discuss and find common approaches and innovative solutions to data policy and data related initiatives and strategies. This has not always been the case with different Government regulators and bodies sometimes recommending contradictory approaches to digital regulation, for example the ICO Direct Marketing Code and policy suggestions produced by the CMA in the Online platforms and digital advertising market study.

Putting in place a more coordinated, systemic approach would enable the UK government to become a global pioneer. For example, in establishing regular feedback loops to allow common problem or issues around the interpretation or application of data protection rules to be identified and policies to be updated, or their interpretation changed, more regularly as and when appropriate.

2. Increasing trust through a meaningful and proportionate approach to data protection

The UK has the opportunity to become a global leader through providing clarity and certainty on the interpretation of current laws and requirements. Rather than introducing new laws, the purpose is to remove friction and inconsistencies and bring clarity to make it easier, not harder, for organisations to comply.

The UK should also look to show the rest of the world how the development of clear guidance and advice can provide clarity to organisations on how to comply in a way that is both meaningful and focused on achieving the overall objectives of data protection law.

This will help the UK become a place where data protection oversight provided by the regulator is not solely focused on issuing fines but in supporting organisations to do compliance well.

This can be achieved by taking steps in the following areas:

> **Bringing clarity and certainty to existing rules**

> **Making the paperwork of privacy more meaningful**

> **Having a regulator that provides certainty and supports compliance.**

Bringing clarity and certainty to existing rules:

A key issue is how the UK's data protection oversight regime can continue to support and guide organisations to better understand existing data protection requirements and achieve the overall outcomes of data protection laws. The goal should be for the UK to become the best place in the world for demonstrating how laws and rules can be interpreted and followed and making it easier rather than harder for organisations to comply.

The UK should look to become a global leader in providing legal clarity and certainty on how fundamental aspects of current data protection laws should be interpreted and applied by the development of clear guidance and advice created in partnership and through consultation with industry. This is not about introducing new legal requirements but showing the rest of the world how existing rules on data protection could be applied in a way that provides clarity and certainty.

Areas where the development of guidance with industry engagement could provide legal clarity and certainty on increasingly complex, difficult and burdensome areas of the current legal framework include the following:

> Ensure that the legal basis for processing data is truly put on an equal footing and there is clarity about how different legal bases can be used in combination to offer a range of services

> Developing a clear and robust understanding of the legitimate interest balancing test and the documentation required to demonstrate compliance (including where the use of DPIA's is needed and where the use of a Legitimate Interest Assessment (LIA) could be used). This would help support the use of this test while also supporting organisations to demonstrate compliance.

> Getting right the interpretation of the purpose limitation principle

> Permitting the use of biometric data where individuals are not being identified or authenticated and facial recognition technologies in different contexts/ circumstances

> Complying with data portability requests particularly in complex situations

> Increased data sharing across government to deliver more effective public services

> Applying a risk-based approach to the anonymisation of data, with clear guidance on specific circumstances where anonymisation would be required.

Guidance is already a key area of the ICO's current work. The Direct Marketing Codes of Practice and Right of Access draft guidance are examples of this. In the development of Codes and guidance, the ICO's use of case studies helped to bring clarity on otherwise complex legal issues. However, it is suggested that the ICO could also look to be more pioneering in the way it provides guidance to help companies explore different ways to achieve outcomes. For example, finding ways to highlight not just good practice examples of compliance but examples of bad practice as well as examples that should be seen as world leading.

One area which offers the UK an opportunity to take a leading role in championing an innovative approach to developing clarity and certainty is in its international data transfers regime.

This is an area where government thinking is needed to shape a more innovative and pioneering approach to better enable international data transfers. For example, as the UK considers its new international data transfer regime, there is an opportunity to consider possible innovative ideas that could streamline or bolster the tools that already exist. Such as:

- How might the process of agreeing BCR arrangements with organisations, or sectors, be fast tracked or just generally improved?
- How can we make Standard Contractual Clauses (SCC) more user friendly for smaller businesses?
- How can codes of conducts as a basis for transfers be made meaningful?
- How might consent and other contractual terms be better used to provide a legal basis in exceptional or ad hoc circumstances?

Making the paperwork of privacy more meaningful

Since the introduction of the UK GDPR, organisations have spent time and resources developing and implementing data protection policies, procedures, and technical solutions in order to comply with the updated law. This has led to an increase in the administrative procedures and paperwork generated by organisations.

Processes have an important role, helping organisations to demonstrate, and provide auditable evidence, for compliance. For example, in relation to the principle of accountability demonstrating compliance remains vital.

However, the purpose of data protection is to protect people's privacy, not generating more bureaucracy which requires significant resources by organisations. The administrative steps taken by organisations must therefore not become simply a tick-box exercise, but be meaningful and help organisations achieve the overall objective of protecting privacy.

To be clear, this is not about reducing levels of data protection or lowering standards.

The goal here should be to explore where current administrative requirements which do not provide meaningful support or help to achieve the highest levels of data protection, could be reformed or removed. For example, the following are suggested requirements within UK GDPR and UK Data Protection Act which should be explored:

> **Article 30 "Record of Processing Activities"** – This requirement involves the creation of large amounts of duplicated paperwork that are already covered within DPIAs and Privacy Notices.

> **Article 14 "Information to be provided where personal data have not been obtained from the data subject"** – This requirement can involve additional administrative tasks for organisations that seems to go against a core principle of the UK GDPR data minimisation.

> **Data Protection Act 2018 Schedule 1, Part 4 Sensitive data policy document** - This requirement involves the restatement of information that organisations may have already provided and recorded through compliance with other requirements and therefore is repetition and duplication of information that exists elsewhere.

Government should conduct an analysis of the current administrative requirements under the wider UK data governance legal framework including the DPA18, UK GDPR and PECR. This should assess where the paperwork being required is providing meaningful support to the objectives of UK data protection laws and identify where current administrative requirements could be streamlined to help businesses focus their resources.

This assessment should also identify areas where a more innovative approach, such as using cutting edge technologies including blockchain, AI and automation, could help to meet the same objectives. This work should explore areas where additional, or duplicated, data protection and privacy regulatory requirements are experienced by specific industries under sector specific laws. For example, the requirement being faced by the telecommunications industry under both the PECR which sits alongside the UK's Data Protection Act and the UK GDPR.

Having a regulator that provides certainty and supports compliance:

A key strength for the UK is the experience, expertise, and reputation of the ICO. It is seen around the globe as a respected, well resourced, world leading data protection regulator. Now is the opportunity to consider how and where the ICO could be even more effective as a regulator that can support, guide, oversee and enable frictionless and meaningful compliance with data protection laws.

As the UK looks to create a national approach and system for data protection that is increasingly joined up, coordinated, pragmatic, modern and pioneering the ICO has a vital role to play. The ICO will be key in providing expert advice and clear guidance to government, regulators, policy makers, industry and other key stakeholders on how current rules should be understood, interpreted and applied. By providing regulatory certainty the ICO can support the UK's goal of being a leader of a modern, agile, flexible and innovative data protection system and regime that supports and encourages cutting edge innovation and builds meaningful data trust and confidence.

As government thinking about how such a system and regime could be built develops it is important that the ICO is involved in this thinking.

It is important that the structures and practices that will need to be put in place to support a more systemic UK approach to data protection that is modern, agile, and innovative are identified. This will mean a clear role for the ICO resources will need to be focused on providing government and industry with legal and regulatory clarity through the development of guidance, advice, enforcement and oversight.

3. Becoming a leader in the global debate on data

The processing of personal data is at the heart of global discussions on trade and innovation, increasing its salience as a key issue of geo-political importance. Organisations including the UN, G7, G20, OECD and WTO have all highlighted data governance as key to their agendas. The EU is proposing its own Data Governance Act as well as reviewing the international data transfer mechanisms under the GDPR. Around the world digital trade rules are becoming a regular feature in trade agreements and at the multilateral level.

Into this debate the UK enters as a newly independent market, the world's third largest digital economy measured by global investment in tech and a significant exporter of digitally delivered services, estimated at around £190.3bn a year with a trade surplus of £99.2bn.[2]

The rules governing digital, data and the protection of personal data are therefore of strategic importance to the UK, and in a contested space this means that the UK Government must become an active participant in supporting a harmonised international regulatory system for data that favours innovation and reduces barriers to trade. The UK's Presidency of the G7 in 2021 provides an opportune moment to make our mark in this debate.

However, as the UK begins managing its own data protection and transfers rulebook, we enter a global landscape with a trend towards data localisation.

As well as China, other countries have begun taking similar steps which can have the effect of market barriers. Recent action by Indonesia allows it to impose tariffs on digital products and the Indian Government aims to grant itself powers to enact discriminatory local data storage requirements and target foreign e-commerce firms and user platforms.

In Europe, the Schrems II ruling has put the EU's current regime for international transfers in doubt with some DPAs calling for EU citizens' personal data to be stored in the EU creating deep uncertainty over how data can be transferred in and out of the bloc.

There is no quick fix to this trend towards data localisation, however the UK can seek to work with others to turn the tide, there are three parts to this strategy:

> **Credibility;**

> **openness;**

> **and leveraging our alliances to create pathways for sharing data.**

[2] Understanding and measuring cross-border digital trade – Department for International Trade 2020

Credibility

The UK should look to lead by example through its domestic regime, guiding and influencing global thinking about the future direction of data governance by showcasing and demonstrating how to develop a trusted data protection framework that encourages innovation as outlined earlier in this paper.

This will also mean ensuring we walk the walk and talk the talk, by taking a tough line on data localisation at home as well as abroad.

At the global level, a UK strategy should seek to champion pathways between high standard data protection regimes, while seeking to shape global schemes and codes of conduct to create routes for private companies, researchers, and others to exchange data in a secure and trusted way.

Engaging in these debates will mean taking a pragmatic view of the global arena on data transfers. The UK already has a strong data protection platform in the UK GDPR and we should seek to build on that model.

To ensure the widest possible opportunities for UK international transfers. This will mean seeking to balance between our approach to international transfers with commitments in free trade agreements, and through new transfer tools such as UK SCCs, BCRs and codes of conduct.

This will be tricky and will require explainable frameworks and toolkits to help companies identify the best and most appropriate way to transfer data with different jurisdictions. Arrangements such as adequacy will be the easiest ways for companies to transfer data, but in their absence the UK must provide businesses with secure and high standard tools to allow for transfers as well as effective guidance to help smaller firms navigate the tools available to them.

The UK is already seen as a respected voice and leader in the global discussion on data protection. The ICO's current leadership of the Global Privacy Assembly is an example of where the UK is leading the global data governance debate and we should seek to further engage in other such forums.

Openness

As an EU Member State, the UK argued for a more pragmatic and open approach to international data transfers. Now that we are outside the Single Market and Customs Union, we must put this into practice.

This means the UK should aim to provide a suite of new transfer tools to complement the existing set we have adopted from the EU to provide businesses with more options.

A more flexible approach would allow companies to continue to use the transfer arrangements they inherited from the EU, but also provide options for companies based in the UK to expand into other markets that they would not have access to if they solely relied on EU transfer tools. The UK would not be the only country to do this. Similar approaches have been taken by Japan and New Zealand where transfer tools were blended with their commitments in free trade agreements to create a variety of options for firms.

For example, UK SCCs, BCRs and guidance set by the ICO should provide an alternative mechanism for transfers, rather than being limited to relying on EU tools. Companies will have to be careful with what data is transferred, but they will have the tools if there is a business case for it.

Guidance from the ICO will also been needed here to ensure businesses understand what they need to do to take advantage of this more flexible system.

Providing new pathways such as UK SCCs, codes of conduct, sectoral adequacy decisions and commitments in free trade agreements will open up new business possibilities for UK companies. This will provide a comparative advantage for basing a business in the UK and demonstrating how a suite of transfer tools and pathways can help companies exchange data with a wide range of partners, not just the EU, but also the US, Australia and other key markets.

In doing so, however, the UK cannot not lose sight of the need for high data protection standards. While we should aim to permit the use of a variety of high standard transfer tools we cannot allow for a situation where trust is undermined. Otherwise, the UK will be seen as a place where personal data is not secure, this would ultimately mean losing data adequacy with the EU and other partners as well as a general loss of trust in our approach.

Leveraging our alliances

Beyond establishing a suite of transfer tools, the UK should aim to engage at the multilateral level to promote common principals, tools and data protection practices which enable pathways for global data to flow.

The UK has a key role, working with our close partners in the EU and US, but also building new alliances such as with Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) countries, and the Commonwealth. At the multilateral level, the UK must continue to show global leadership as a convener and facilitator of the global conversation about the future of data protection and privacy issues, for example through forums such as the G7, G20, OECD and WTO. Arguably this is of even greater importance now in order to counteract any trends towards data localisation within trading blocs.

It is unrealistic to think that we will be able to converge data protection standards across the world to create truly free data flows. Not least because even where the same rules exist there are often large differences in how these are practically applied, meaning there will likely always be some safeguards between jurisdictions.

However, by seeking to promote common principles between countries, and regional blocs, we can ensure that we are fostering a harmonised global regulatory framework which will enable UK businesses to continue to benefit from the global digital economy.

The UK's presidency of the G7 this year provides a prime opportunity to take the reins of leadership in this debate. Seizing this opportunity and being an active participant in these debates would also help position the UK as the place where innovators come to engage in the most difficult, tough questions about the role of data and how to get data protection right as technological innovations, such as facial recognition, are developed, tested, and deployed.

The UK's leadership in digital ethics, and creation of bodies such as the Centre for Data Ethics and Innovation (CDEI), already demonstrates how the UK is already considered a global leader in these debates and discussions. The Government can capitalise on this by examining how the UK's approach to exploring and addressing data and digital ethics issues could be shared and replicated through global forums and bilateral relationships.

This will not only give the UK a new role in international relations but make it an attractive hub for leading companies to develop products and champion new approaches to data protection.

techUK
FOR WHAT COMES NEXT

About techUK

techUK is a membership organisation that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. We collaborate across business, Government and stakeholders to fulfil the potential of technology to deliver a stronger society and more sustainable future. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

linkedin.com/company/techuk

@techUK

youtube.com/user/techUKViews

info@techuk.org