Department for Science, Innovation & Technology

Viscount Camrose
Parliamentary Under Secretary of State
Department for Science, Innovation & Technology
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dsit

24th April 2024

House of Lords
London
SW1A 0PW

My Lords,

Thank you for your continued engagement with the Data Protection and Digital Information (DPDI) Bill during the fourth and fifth days of Committee stage. I am writing to follow up on questions raised by Noble Lords during the debate, to which I have provided a more detailed response below. I am copying this letter to all noble Lords who were present during the fourth and fifth days of Committee stage and will deposit a copy in the House Library.

Enforcement action for violations of international transfer rules

I will first address Lord Bethell's request to share examples of cases where the ICO has acted against breaches of UK law on international data transfers.

Although it would be inappropriate for me to comment on how the ICO exercises its enforcement powers, it should be noted that the ICO took enforcement action against Equifax Ltd in 2018 with a monetary penalty notice totaling £500,000 – doing so, in part, due to an international transfer breach. The Government has introduced a new requirement on the ICO in this Bill to publish an annual report on how it has exercised its enforcement powers. This will provide greater transparency and accountability to the ICO's exercise of its enforcement powers.

The UK has strong safeguards and enforcement regimes to ensure that personal data is collected and handled responsibly and securely. This is not changing with the reforms to the UK's international transfers regime for general processing which maintain high

standards of data protection when data is transferred outside of the UK. Companies operating in the UK are required to comply with our data protection legislation when transferring UK data overseas. Failure to do so, including when obligations to put in place appropriate safeguards under Article 46 UK GDPR are not fulfilled, can result in ICO enforcement action and the ICO has powers to conduct investigations, issue fines and to compel companies to take corrective action.

The DPDI Bill also consolidates provisions containing an existing power for the Secretary of State to restrict, by regulations, transfers of categories of personal data to other countries or international organisations where necessary for important reasons of public interest. Similarly, the ICO will continue to have the power to order the suspension of data flows to a recipient in a third country or to an international organisation. Cross border regulatory enforcement and cooperation is a key tool to ensuring personal data is sufficiently protected, and the ICO has joined a new international multilateral agreement with the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE) alongside the United States, Australia and others.

Researcher's access to data

I will now turn to Baroness Kidron's queries about Ofcom's role in regulating researcher's access to data.

a. Ofcom Codes of Practice

Baroness Kidron asked whether Ofcom codes and mitigation demands will be based on current practice of tech companies.

As the online safety regulator, Ofcom is required to set out the steps that providers can take to fulfil their Online Safety Act (OSA) safety duties in codes of practice. The intention is that the steps that Ofcom recommend should be suitable to mitigate the risks of harm to individuals arising from in-scope illegal content and content that is harmful to children, as identified in providers' risk assessments, and to enable providers to fulfil their other duties in the Act. These steps should also be proportionate to different providers' size and capacity and the risk of harm as identified in Ofcom's risk assessment. They also need to be technically feasible for providers to implement. The OSA does not distinguish between steps based on current industry practice or which are different from current industry practice. Ofcom may recommend whichever steps are best suited to fulfilling the above requirements.

To note, these are the first iteration of Ofcom's codes of practice. We anticipate that these codes will evolve over time as Ofcom develops its evidence base. Many of the measures

that Ofcom has proposed in this first version of the illegal harms codes will improve safety standards across the industry. This includes areas such as: governance and risk management, hash matching for CSAM, grooming, improved reporting and complaints mechanisms and fraud measures.

b. **Use of external evidence for Ofcom proposals**

Baroness Kidron also asked for clarity on whether whistleblowers, NGO experts and evidence from user experience could be used to guide regulators. She also raised a separate query about whether EU research done under the auspices of the Digital Services Act (DSA) would be considered adequate, if the concerns overlapped with UK law.

Ofcom is statutorily required to consult on its proposals for how providers should approach their safety duties and their other duties under the Act. In exercising their online safety functions, Ofcom will take into account any relevant evidence. Ofcom will have the power to gather the information that they require and use their judgment as an independent regulator in assessing evidence. Interested parties can submit evidence to Ofcom as part of these consultation processes. These include the kinds of individuals and organisation mentioned in the question. Ofcom can take these submissions as evidence when drafting its codes of practice.

c. Risk mitigation

Baroness Kidron asked for more information on how Ofcom should mitigate any identified risks for which no current measures are in place.

Under the OSA, providers must carry out an assessment of in-scope risks and implement safety measures to mitigate the risks of harm to individuals who encounter in-scope illegal content. For example, under their illegal content duties, providers need to do an assessment of the risk that UK-based individuals will be harmed as a result of users encountering in-scope illegal content on their services. Or as a result of their services facilitating other kinds of illegal offending, providers must then implement safety measures to mitigate the risk of harm to individuals deriving from this content and activity. These duties are proportional to the risk of harm as well as to each providers' size and capacity, among other factors.

Ofcom will set out steps in codes of practice that providers can take to fulfil these duties, which can include the steps providers can take to mitigate risks on their services, and to fulfil their safety duties Ofcom has begun this process by setting out measures providers can take in their draft illegal content codes of practice. It published these for consultation in November last year and the consultation closed in February.

The Government is working closely with Ofcom to ensure the regime is implemented in full as soon as possible. Ofcom's approach to implementation can be accessed here: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/270215/10-23-approach-os-implementation.pdf.

d. Support for academic researchers

Baroness Kidron also questioned whether new measures for testing and sandboxing of AI models would allow academics to access data for research, independently of government and tech. On a related note, she asked how government would support academics to access data to study online safety and privacy.

The AI Safety Institute (AISI) is the world's first state-backed organisation focused on advanced AI safety for the public benefit and is working towards this by bringing together world-class experts to understand the risks of advanced AI and enable its governance. The AI Safety Institute will establish clear information-sharing channels between the Institute and other national and international actors. These include policymakers, international partners, private companies, academia, civil society, and the broader public.

The Online Safety Act improves the information that is available to researchers by empowering Ofcom to require major providers to publish a broad range of online safety information through annual transparency reports.

Ofcom will also be able to appoint a skilled person to undertake a report to assess compliance or to develop Ofcom's understanding of the risk of non-compliance and how to mitigate such a risk, which may include the appointment of independent researchers as "skilled persons". Further, Ofcom is also required to conduct or commission research into online harms and has the power to require companies to provide information to support this research activity.

ICO Complaints and Redress

I will first address Lord's Bassam's request to provide details of the consultation on the complaints and redress procedure for breaches of data protection law and, and then turn to Lord Clement-Jones's request for more information on the government's position with respect to the distribution of data protection cases between courts and tribunals.

The government undertook a thorough consultation process to review the operation of the provisions in Article 80(1) of the GDPR, enabling data subjects to permit certain representative bodies to bring complaints or claims on their behalf and the merits of further enabling such representative bodies to pursue complaints or claims independently of a data subject's mandate. Section 189 of the Data Protection Act 2018 mandated and defined the parameters for this review. Between August 27th and October 22nd, 2020,

the government issued a Call for Views and Evidence, inviting stakeholders to submit their perspectives and relevant information.

During this consultation period, the government received a total of 345 written responses from various organisations and individuals. These responses came from a diverse range of stakeholders, including privacy rights campaigners, children's rights organisations, academics, parent and child advocacy groups, trade associations, individual businesses, and regulators.

In tandem with the written submissions, government officials conducted numerous meetings with a wide range of stakeholders. These included engagements with privacy rights campaigners, children's rights organisations, academic institutions, groups advocating for parents and children, trade associations, individual businesses, and regulators. Furthermore, officials actively sought the perspectives of young people by collaborating with youth groups in Manchester and London.

You can find a copy of the government's call for views and its response to the consultation here. The response includes a complete list of the organisations that responded to the call for views, and it also provides details on the number of cases received by the ICO at the time and how they are distributed.

Having considered the evidence, the government concluded there was not a strong enough case for introducing new legislation enabling bodies to represent data subjects without their mandate. Although the government accepts that some groups in society might find it difficult to complain to the ICO or bring legal proceedings of their own accord, there is no strong evidence to suggest the ICO cannot or will not investigate serious breaches of the legislation that are brought to their attention. The Government's primary interest is in a regulatory system that effectively protects individuals' personal data, including those of children and vulnerable groups. Based on the available evidence, there is no clear case that the current legislative and supervisory arrangements, including the existing routes of redress, are not delivering on this objective.

I turn now to the government's position in relation to the distribution of data protection cases between courts and tribunals, in response to the question from Lord Clement-Jones.

As the noble Lord is aware, there is currently a mixture of jurisdiction for tribunals and courts in relation to data protection proceedings. Generally, statutory appeals against public bodies are dealt with by Tribunals – for example, appeals against a national security certificate (under sections 27, 79 and 111 of the DPA 2018), appeals against an investigative or enforcement notice from the Information Commissioner (under section

162), or an application for an order for the Commissioner to take steps to respond to a complaint (section 166). Usually, such proceedings are handled by the First-Tier Tribunal with the Upper Tribunal hearing any appeals.

Court proceedings, on the other hand, tend to be reserved for claims for damages by data subjects against controllers and processors (most notably under Article 79 of UK GDPR and section 167 of the DPA 2018) and applications by the Commissioner for particular orders (for example, under section 145 of the DPA for an order for a person to provide them with information). Claims for damages are generally handled by the County Court but may be transferred to the High Court in some cases (see rule 30.3 of the Civil Procedure Rules). Where no other remedies are available, claims against public authorities can be brought to the High Court for judicial review, in cases where, for example, the public authority acts outside its powers or makes any other errors of law in its decisions.

The government is confident that the current system is balanced and proportionate and provides clear and effective administrative and judicial redress routes for data subjects seeking to exercise their rights.

Digital Verification Systems (DVS)

Lord Clement-Jones also raised two queries about DVS, the first requesting more detail on the relationship between the DVS framework and Gov.UK One Login.

The GOV.UK One Login programme is building a digital platform which gives people a single way to sign in and prove (and reuse) their identity to access government services. In contrast, the measures in this Bill are focussed on creating a framework to enable the confident use of secure and trusted digital identity solutions in the wider economy. It will enable people to digitally prove things about themselves with confidence.

The measures in the Bill achieve this aim by allowing organisations to have their services independently certified against the trust framework to prove they are providing secure and trustworthy digital verification services. The trust framework, as you will recall, is a collection of rules, best practice, and standards for digital verification services in the UK which has undergone four years of development, consultation, and testing within the digital identity market (the beta version can be found here). The interaction between GOV.UK One Login and the DVS framework is that GDS is working with DSIT to ensure that GOV.UK One Login aligns with the trust framework in that both are trusted to produce secure and reliable information while protecting users' interests.

Each programme relies on distinct information sharing powers specific to their respective purposes. Information sharing between public bodies, including in support of GOV.UK One Login, is enabled by the Digital Economy Act 2017 and is specific to the provision of public services. In context of this Bill, the DVS framework enables registered DVS providers to make verification checks against information held by public authorities. The request for such information sharing must always originate from the individual to whom such data relates.

Lord Clement-Jones' second concern was about whether the police have been provided with guidance on existing criminal offences that cover situations where an individual's digital identity is misused or used without their knowledge to carry out a digital transaction. I noted during the debate that this issue falls under the domain of the Home Office, but I am happy to provide you with further information. For your information, I have listed below the relevant clauses in current legislation that could apply in such circumstances:

- Under Section 2 of the Fraud Act 2006 of making a false representation intending to make an unlawful gain or cause (or risk) a loss to another person; or
- Under Section 1 of the Computer Misuse Act 1990 of causing a computer to perform a function to secure unauthorised access to program or data held in a computer.

In addition, there are offences under section 170 of the Data Protection Act 2018 covering the deliberate or reckless obtaining, disclosing, procuring and retention of personal data without the consent of the data controller.

In terms of guidance offered to policing, the Home Office and College of Policing are currently reviewing the fundamental training offered to police officers relevant for fraud, including digital skills. In addition to this, we recognise the harm caused by identity theft to victims and have included it as part of the Independent Review into disclosure and fraud offences. Chaired by Jonathan Fisher KC, Part 2 of the Review, which is due to report in 2025, it will consider if fraud offences meet the challenge of investigating and prosecuting fraud.

Inclusive access to services

During the debate, Noble Lords raised the issue of access to services and concerns that individuals might not be able to access certain services if digital verification services were the only method of proving their identity and queried how the Equality Act 2010 may play a role in addressing such issues. I would like to clarify my statement and provide additional context in this area.

The government is committed to enabling the use of trusted digital identity solutions to help make people's lives easier and allow them to prove things about themselves safely and securely. As we discussed, digital identities will not be mandatory, and people will still be able to prove things about themselves using physical documents. But for those who wish to use them, the government's intention is that digital identity products are inclusive; anyone who wishes to use a digital identity should be able to get one and use it. We consistently engage with civil society groups to receive their expert feedback on how to increase inclusion as we develop the policy.

The Equality Act 2010 protects individuals from discrimination in the provision of goods and services in both the private and public sectors. The Act does not create an absolute entitlement for goods or services to be provided in any particular form or manner; but service providers must ensure that they do not unlawfully discriminate against individuals on the basis of their protected characteristics in the provision of those services. The Act does require that organisations make 'reasonable adjustments' to make their services accessible. This therefore applies to DVS providers and the organisations that rely on those services, such as banks.

In addition, the Public Sector Equality Duty places an additional requirement on public authorities to have "due regard" to the need to:

- eliminate unlawful discrimination, harassment, victimisation and any other unlawful conduct prohibited by the act
- advance equality of opportunity between people who share and people who do not share a relevant protected characteristic
- foster good relations between people who share and people who do not share a relevant protected characteristic

As a result, the availability of non-digital routes is something that public authorities already routinely consider in the provision of public services. The trust framework beta, the link to which is provided above, outlines how to improve inclusion and encourages companies to adopt practices such as choosing technologies which have been tested with users from a variety of demographics.

I will be hosting a series of engagements as usual after Committee stage and before Report; I look forward to discussing this further with you then.

Adequacy and reporting

In response to questions regarding independent expert views on potential adequacy risks, I would like to reassure the Noble Lords that, since the beginning of the process to reform our data protection laws, the Government has continuously engaged with a wide range of stakeholders on the interaction of the proposals in the DPDI Bill with EU adequacy.

This includes our consultation process in late 2021, which attracted 2,924 responses that provided valuable feedback on how to maintain high data protection standards and highlighted the importance of the free flow of data with the EU. The Government's response to the consultation, including a list of respondents can be found here. The Government carefully considered these suggestions when designing these reforms and, in 2023 subsequently reintroduced the Bill following a detailed codesign process with industry, business, privacy and consumer groups to determine how we could improve the Bill further.

In January 2022, the Government also launched the International Data Transfers Expert council, bringing together 20 world-leading data experts from across academia and industry representative bodies to advise the Government on data flows issues. The Council's recent independent report recognised the importance of adequacy.

Below I outline views provided by stakeholder groups that we have engaged with, the majority of whom share our view that our reforms are compatible with maintaining EU adequacy.

House of Lords European Affairs Committee inquiry on EU-UK data adequacy

As part of its ongoing inquiry on EU-UK data adequacy, the European Affairs Committee has heard to date from five prominent data privacy experts and practitioners as well as the Information Commissioner. All these stakeholders highlighted the importance of the UK maintaining its EU adequacy decisions and believed the reforms in the DPDI Bill will achieve this.

Mr **Joe Jones**, Director of Research and Insights at the International Association of Privacy Professionals and former Deputy Director for International Data transfers at the Department for Digital, Culture, Media and Sport, noted during the inquiry:

"*My strong sense is that the reforms have been designed with a view to retaining EU adequacy."*

“Within the current parameters of what is being considered and proposed in that Bill are things that do not go to the heart of essential equivalence.

Ms **Eleonor Duhs**, Partner and Head of Data & Privacy at Bates Wells, argued the UK’s regime will remain close to the EU’s post reform but cautioned that reforms to the Information Commissioner’s Office may be scrutinised by the Court of Justice of the European Union in the event of a legal challenge:

“The European Commission would do everything it could to continue data adequacy for the UK. EU businesses will want to be able to send data freely to the UK without having to put standard contractual clauses and risk assessments in place. One of the issues for the European Commission is that, if the UK does not have adequacy, the bar is set almost impossibly high for any other country. Even with the Data Protection and Digital Information Bill, our data protection framework will be very similar to the EU’s.”

From a trade association perspective, Mr **Neil Ross**, Associate Director for Policy at TechUK, shared his view that the risk of the DPDI Bill to EU adequacy is low:

“The reforms that the UK is planning to put in place through the data protection and digital information bill have been well consulted with the European Commission and the fact that the UK is now planning to operate within this broad framework, I think the risk of losing adequacy is quite low.”

“In reality [the DPDI Bill] is a carefully calibrated evolution not revolution of the data protection regime which basically aims to make things a bit more flexible to update the law for new technology and make it easier in particular for small business to comply. So this seems like a natural evolution in the law and therefore we are in quite a good place.”

“The EU is already looking at for example, how when the DPDI Bill is implemented, how it might then inform an update to the GDPR in the European Union and those discussions are ongoing. The first thing I would say though is, the design of the DPDI BILL is quite strange as legislation, it’s designed to both be new but also completely interoperable with the GDPR. All the indications are that they will assess that the UK is maintaining an essentially equivalent level of data protection level to the EU GDPR.”

Regarding the possibility of a legal challenge at the CJEU, Mr Ross added:

“For the DPDI Bill that’s broadly going to be fine even if a challenge came. If you struck down the DPDI Bill’s provisions as being non-adequate it would have a whole cascade of effects across the world because no other country would be at that standard.”

Ms **Bojana Bellamy**, President of Centre for Informational Policy Leadership and independent expert of the DSIT International Data Transfer Expert Council highlighted:

“There is no doubt, in my opinion and in the opinion of many organisations, that adequacy is helpful and should be retained.

[...] It would be detrimental to European businesses if there were to be a finding of lack of adequacy, because they would have to go through all these processes of paperology and legal papering data flows to the UK. If you speak to the likes of SAP, BNP Paribas, Accord, big players, telefónicas, German companies, the automotive industry, none of them really want that. It is not in their interests either.

I think it is possible but highly improbable.”

In addition, when providing evidence during the DPDI Bill’s House of Commons Committee Stage in May 2023 Ms Bellamy stated that:

“I do not believe there are elements of the Bill that would reduce adequacy; if anything, the Bill is very well balanced.”

Mr **Zack Meyers**, Assistant Director at the think tank the Centre for European Reform also considers:

“Compared to a few years ago, when I thought that the stability of the data adequacy arrangement between the UK and the EU was questionable, I think that things have become a lot more certain [...] the relationship between the UK and the EU has dramatically become much warmer and more constructive compared to a few years ago. That makes it less likely that the Commission will be interested in upsetting adequacy. [...] There is some evidence that the Commission has been a bit worried that if adequacy becomes such a high standard to meet that it is nearly impossible for other countries to meet it, in practice countries will give up on meeting EU standards entirely”

The Information Commissioner Mr **John Edwards** retained his view that the DPDI Bill does not pose a risk to EU adequacy:

"I challenge any colleague in Europe to take the Bill as is now before Parliament and compare it with the GDPR as enacted in European jurisdictions and to find another regime among the other 15 adequate countries that is more similar than the UK is to Europe. If there is a risk, it is a risk based on political machinations rather than on principled analysis."

In his response to the DPDI Bill's reintroduction, the Information Commissioner further added: "*Adequacy does not require a carbon copy of the GDPR and these changes maintain the high standards that both the UK and EU are committed to...In my view the proposed changes in the bill strike a positive balance and should not present a risk to the UK's adequacy status."*

DPDI Bill House of Commons Committee Stage

Prior to the European Affairs Committee's inquiry, additional experts provided supporting views and feedback during the DPDI Bill's House of Commons Committee Stage in May 2023.

These include Mr **Eduardo Ustaran**, Partner at law firm Hogan Lovells and member of the Government's International Data Transfers Expert Council. Mr Ustaran affirmed:

"It is really important to note at the outset that the changes being proposed to the UK framework are extremely unlikely to affect that adequacy determination by the EU, in the same way that if the EU were to make the same changes to the EU GDPR, the UK would be very unlikely to change the adequacy determination of the EU. It is important to appreciate that these changes do not affect the essence of UK data protection law, and therefore the adequacy that is based on that essence would not be affected."

Ms **Vivienne Artz**, Former Managing Director and Chief Privacy Officer, London Stock Exchange echoed these supportive statements:

"I concur; I do not think the Bill poses any threat to adequacy with the EU [...] There is nothing in this Bill that would jeopardise adequacy with the EU."

Jonathan Sellors, Legal Counsel, UK Biobank, spoke from a legal perspective stating:

"I think it is absolutely right to be concerned about whether there will be issues with adequacy, but my evaluation, and all the analysis that I have read from third parties, particularly some third-party lawyers, suggests that the Bill does not or should not have

any impact on the adequacy decision at all."

Other

Since the introduction of the DPDI Bill several academics, experts, practitioners, trade associations and civil society groups have provided independent views on the effect of the DPDI Bill on EU adequacy with widespread support for the UK's reforms.

In an opinion piece from March 2023 for law firm Allen & Overy, former Deputy Information Commissioner and special advisor to the European Affairs Committee's inquiry, Mr **Steve Wood** wrote:

"In our previous blog, we considered the implications for adequacy and concluded that the original Bill did not create a strong risk to the UK's adequacy status with respect to the EU."

In September 2023, academics from the **LSE Law School** and **Maynooth University** produced a report for Northern Ireland Department for the Economy assessing that the European Commission will likely seek to renew its adequacy decisions for the UK but that a challenge at the Court of Justice of the European Union may risk EU adequacy.

The Noble Lords also asked me to include in this letter the opinions of stakeholders who are not supportive of the Bill. Some civil society organisations have provided critical, and in the Government's view inaccurate, claims that these reforms will lower data protection standards in the UK and have called for the European Commission to reassess its decisions and take action if deemed appropriate. These calls culminated in a open letter to the European Commission in July 2023.

Biometrics

Viscount Stansgate asked me for reassurance that there will be sufficient reporting to Parliament from the various bodies taking over from the Biometrics and Surveillance Camera Commissioner.

In response to the outcome of the Data Reform public consultation in 2021, we are reforming the oversight landscape for biometrics and surveillance cameras by abolishing the roles of the Biometrics and Surveillance Camera Commissioner, and the Surveillance Camera Code. This is because the public and the police stated they found the current oversight framework complex and inefficient due to the overlaps between the many

bodies that operate in this space. We are seeking to address the duplication of roles and responsibilities by simplifying the oversight landscape.

As I stated in the debate, these reforms won't lead to a gap in oversight as there is existing overlap between the Commissioner and the remit and responsibilities of other bodies, such as the Information Commissioner's Office (ICO), the Forensic Science Regulator (FSR) and the Equality and Human Rights Commission (EHRC). For example, the ICO will continue to regulate the processing of personal data for the purposes of surveillance. His Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) also inspect, monitor, and report on the efficiency and effectiveness of the police. The other bodies providing oversight also have the statutory powers variously to inspect and report, investigate, litigate and set quality standards.

In terms of reporting, the ICO, EHRC and FSR already produce annual reports to Parliament. HMICFRS also publish reports of their inspections. We are undertaking further engagement with these bodies about how they will prioritise reporting on biometrics and surveillance, once there are no longer overlapping oversight arrangements, to ensure there continues to be comprehensive, appropriate reporting of matters relating to biometrics and surveillance in the future.

I also committed to write in relation to Baroness Jones' question concerning Lord Holmes' amendments 197A, 197B and 197C which seek to establish a statutory "Biometrics Office" responsible for overseeing biometric data use, and place new obligations on organisations processing biometric data.

I would like to reiterate that the responsibility for monitoring and enforcing the processing of biometric data already rests with the Information Commissioner and that these functions will transfer to sit with the new Information Commission, once established. Indeed, the Information Commissioner's Office has a long track record of regulating data protection across a wide variety of use cases, and they have already provided guidance, opinions and carried out regulatory action in this area.

Under Schedule 15, paragraph 13 of the DPDI Bill, the Information Commission is enabled to establish committees of external experts with skills in any number of specialist areas, including biometrics, to provide specialist advice to the Commission and inform its regulatory decision making and oversight.

As such, the new governance structure of the Information Commission offers a high degree of flexibility in its approach to the involvement of experts. The government is of the firm view that the Information Commission itself is best placed to continue to oversee the processing of biometric data, and that delegation to a new, separate statutory Office

as set out in the noble Lord's amendment, is unnecessary and would only add needless complexity to the regulatory landscape.

Yours sincerely,

Viscount Camrose
Parliamentary Under Secretary of State at the Department for Science, Innovation & Technology