Explanatory Framework for Adequacy Discussions

Section A: Cover Note

Section A: Cover Note

Introduction

The UK has a world-class data protection regime. The UK Government is committed to ensuring the UK remains a global leader in data protection, working with the Commission and our other like-minded partners to promote strong data protection standards across the world. **Protecting personal data is and will continue to be a priority for the UK.**

The continued free flow of personal data is vital for the future relationship between the UK and the EU. Imports and exports of both goods and services heavily depend on the free flow of personal data between the UK and the EU. EU personal data-enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018, and exports from the UK to the EU were worth £85bn (€96bn).[1]

Given these economic ties and our shared commitment to high data protection standards, the Government believes it is in both parties' interests to act quickly to ensure the reciprocal free flow of personal data between the EU and the UK. The UK Government stands ready to assist the Commission in undertaking an assessment to allow the adoption of adequacy decisions for the UK and Gibraltar. We have made arrangements to allow for the free flow of UK personal data to the EU.

This comprehensive pack of explanatory material provides the information necessary for the Commission to plan and conduct its assessment in good time. It also contains explanatory material about the data protection framework in Gibraltar, put together by officials in the Government of Gibraltar. As the UK's and Gibraltar's legislative and regulatory frameworks are similar – with only minor differences based on domestic considerations – the Gibraltar sections of this pack complement the UK explanatory material by focusing on the areas of difference between the two regimes. The Gibraltar sections of the pack indicate which areas of the UK material should be read as also applying to Gibraltar.

Why the UK meets the standard of "essential equivalence"

The key legislative elements of our framework at the end of the transition period will be the *Data Protection Act 2018 (DPA 2018)*, and the *UK GDPR*. These provide comprehensive protections for data subjects equivalent to those in EU law[2], including:

- ☑ **Robust principles** to protect personal data: lawfulness, fairness, and transparency[3]; purpose limitation; data minimisation; accuracy; storage limitation; integrity and

[1] Estimated by the UK government's Department for Digital, Culture, Media & Sport by applying the UN definition of digitally deliverable services (DDS) to UK Office for National Statistics data.
[2] Part 4 of the DPA 2018 has no equivalent in EU law – it is consistent with the modernised C108.
[3] For law enforcement processing, lawfulness and fairness only.

confidentiality; and accountability. There are also **clear definitions for vital concepts** such as personal data, sensitive data, processing, controller, and processor;

☑ **Clear grounds limiting when processing of personal data is lawful,** including further conditions for the validity of consent. The UK GDPR also sets down additional conditions for processing sensitive and criminal convictions data, and Part 3 of the DPA 2018 sets out the equivalent conditions for law enforcement processing;

☑ **Effective and enforceable rights to give individuals more control over their data**:

- ✓ the rights to request access to their personal data, rectification of their data, and the rights to object to its processing and request its erasure;
- ✓ a right to receive clear information about the processing of their personal data;
- ✓ a right to have the processing of personal data for direct marketing purposes stopped, a right to portability of data, a right to restrict processing, and a right not to be subject to a decision based only on automated processing.

☑ **Limitations and conditions** to ensure that, when restrictions to those rights are provided for through legislation, they are **necessary and proportionate;**

☑ **Clear onward transfer rules** to ensure personal data continues to receive an adequate level of protection when it leaves the UK;

☑ **Additional safeguards** provided in certain situations through requirements such as detailed records of processing, data protection impact assessments, a data protection officer, and data breach notification.

Robust rules require robust enforcement, and the UK's framework provides for <u>effective administrative and judicial redress</u> for data subjects in the UK and the EU. In particular:

☑ The UK's data protection authority, the Information Commissioner's Office (ICO), has **a strong track record** as an **independent** regulator capable of handling complex cases and imposing tough sanctions where necessary. Between 25 May 2018 and 31 December 2019, the ICO received around 23,000 personal data breach reports and closed more than 22,000. In the same period, it issued 71 information notices, 17 assessment notices, and 13 monetary penalties notices;

☑ The ICO has the **power to levy substantial administrative fines** on organisations of up to £17.5m or 4% annual global turnover. The **ICO has been one of the three most**

active data protection authorities in recent years in terms of individual fining decisions[4];

☑ The ICO has a **full range of enforcement powers**, which were expanded by the DPA 2018. These include the power to carry out 'no notice' inspections, without a warrant, by imposing an urgent assessment notice in certain circumstances, and the criminalisation of controllers seeking to frustrate an information or assessment notice by deliberately destroying or concealing relevant evidence;

☑ The ICO is **well resourced**, with approximately 750 staff. This has enabled it to develop **world-leading expertise** in niche areas such as the impact of new technologies and privacy rights, increasing its ability to take effective enforcement action;

☑ The ICO **works closely with other data protection authorities**. The ICO has been the lead/co-rapporteur for 50% of the Article 29 Working Party (now the European Data Protection Board's) guidelines, and the lead authority on dozens of One Stop Shop cases. Many other data protection authorities have re-used the ICO's domestic guidance. **The UK is committed to maintaining this cooperation** going forwards;

☑ The ICO is influential in **driving global privacy standards.** It was a founding member of the Global Privacy Enforcement Network – which now comprises 69 privacy enforcement authorities from across the globe – and the Information Commissioner is currently chair of the Global Privacy Assembly;

☑ In addition to having the right to lodge a complaint with the ICO, data subjects also have the right to **seek judicial redress** against a controller or processor, including compensation. They may also seek a judicial remedy against a decision of the ICO.

The UK's legal framework also sets out <u>robust rules for law enforcement and national security processing</u> of personal data, such as:

☑ Part 4 of the DPA 2018, which governs the processing of personal data by, or on behalf of, the UK intelligence community. This legal framework was designed to be consistent with the data protection standards and obligations provided for in the modernised Convention 108 and helps to ensure that processing by the UK intelligence community continues to be **subject to appropriate and proportionate controls**;

[4] Section G (Role of the ICO and Redress)

- ☑ The Investigatory Powers Act 2016, which is world-leading legislation, provides for **unprecedented transparency and oversight** over the use of investigatory powers in the UK, overseen by the Investigatory Powers Commissioner;

- ☑ Part 3 and Schedules 7 & 8 of the DPA 2018, which, together with provisions in Parts 5 to 7 (DPA 2018) which apply across the GDPR, Law Enforcement and intelligence services regimes), transpose the provisions of the Law Enforcement Directive (LED) into UK law. **This bespoke regime only applies to the processing of personal data for law enforcement purposes**, and is tailored to the needs of the police, prosecutors and other law enforcement agencies. Like the GDPR and Part 4 (DPA 2018), Part 3 is **subject to appropriate and proportionate controls which protect the rights of data subjects and sets out the obligations controllers and processors must comply to, whilst enabling law enforcement officials to continue their important work**.

Together with the rest of the UK's framework, these ensure the activities of UK law enforcement, security, and the intelligence community adhere to **strict principles of necessity and proportionality**.

Ongoing commitment to robust global data protection standards

No matter how strong a data protection law is, it **needs a strong ecosystem that underpins it.** That is why the UK has a wide range of measures that create a digital environment in which citizens can feel safe and secure and have trust in how their data is used.

Our National Cyber Security Strategy sets out ambitious policies to protect the UK in cyberspace, backed by a £1.9 billion investment. Alongside the UK Government's ongoing work towards a National Data Strategy, our plans for a world-leading approach to online safety will play a vital role in strengthening the UK's digital ecosystem. The UK Government has also established bodies to provide advice and leadership on data policy: the independent Centre for Data Ethics and Innovation to advise on ethical and innovative uses of data, as well as the Office for Artificial Intelligence (AI) to tackle the challenges of safely using data to drive forward research and improve people's lives.

Underpinning all of the UK's wider framework, our legal system plays a vital role in the data ecosystem. Our **judiciary is recognised globally for its outstanding fairness and independence**, and its lawyers for their excellence.

The rule of law is integral to the UK constitution. Our courts are universally recognised to be a forum where disputes will be determined on the basis of their intrinsic merits, without regard to the nationality, political persuasions, race, religion, or other characteristics of the parties. The UK has a longstanding tradition of **ensuring rights and liberties are protected domestically** and of fulfilling our international human rights obligations.

Further steps

The UK will work to facilitate the continued free flow of personal data to the EU. This includes a clear, transparent framework to facilitate dialogue, minimise the risk of disruption to data flows, and support a stable relationship between the UK and the EU.

In parallel, the UK looks forward to working with the European Commission and other EU partners to make arrangements for appropriate ongoing cooperation between data protection authorities.

Conclusion

The UK has a long and proud tradition of defending privacy rights. In the 1970s, the UK developed pioneering committees to explore the protection of personal data, and in 1981 the UK was one of the first to sign Convention 108.

More recently, the UK played an active role in developing the GDPR and LED. The UK Government will continue to promote high data protection standards.

The UK puts data protection and trust at the heart of our digitised society. Our ongoing ability to do this will require a world leading and global response that sees us work in tandem, at a domestic and international level, to uphold strong data protection standards that enable the societal and economic promise of data while safeguarding rights and protections.

The UK stands ready to offer further clarifications throughout the assessment process and looks forward to an open dialogue with the Commission.