HM Government

Framework for the UK-EU partnership

Data protection

MAY 2018

Introduction

This presentation is **part of a series produced by the UK negotiating team** for discussion with the EU, in order to inform the development of the future framework.

It **focuses on an element of the vision for our future relationship** set out by the Prime Minister in her speeches in Munich and at Mansion House.

The **future framework will set out the terms of our future relationship**, to be translated into legally binding agreements after the UK's withdrawal.

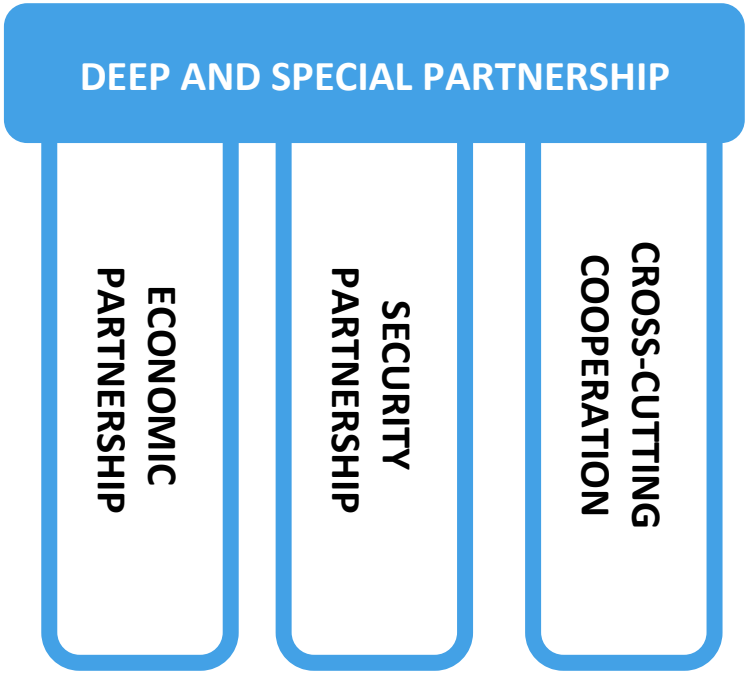
The **UK and the EU will conclude the future framework alongside the Withdrawal Agreement** later this year.

Our vision for the future partnership

The United Kingdom wants to build a **new, deep and special partnership** with the European Union.

It should be a partnership that **protects our shared interests and values**, ensuring we act together for our mutual benefit.

With an approach that delivers for **the whole United Kingdom** and our wider family of overseas territories, as well as for the EU.



This partnership should have **two core parts:**

- An **economic partnership**, that goes beyond any existing FTA, covering more sectors and with deeper cooperation.
- And a **security partnership**, maintaining and strengthening our ability to meet the ever evolving threats we both face.

These will sit alongside **cross-cutting areas** such as data protection.

Structure of discussions on the future framework

The UK and EU negotiating teams have jointly agreed the **structure for discussions on the future framework**, reflecting the breadth of the partnership both sides want to build.

BASIS FOR COOPERATION	Structure, governance, interpretation and application, dispute settlement, non-compliance and participation and cooperation with EU bodies
ECONOMIC PARTNERSHIP	Aims of the economic partnership, goods, agricultural, food and fisheries products, customs, services and investment, financial services, digital and broadcasting, transport, energy, horizontal measures and mobility framework
SECURITY PARTNERSHIP	Aims of the security partnership, law enforcement and criminal justice, foreign, security and defence and wider security issues
CROSS-CUTTING/ STANDALONE	Data protection, cooperative accords (science and innovation/culture and education) and fishing opportunities

The importance of a future relationship to exchange and protect personal data

The continued, uninterrupted and secure flow of personal data between the EU and UK is vital for all partners.

High standards of data protection (based on the GDPR and Law Enforcement Directive) will **underpin all areas of the future relationship**, including the Economic and Security Partnerships.

An agreement on data protection will **be crucial for the EU and the UK**, and any disruption to cross-border data flows would be costly to all partners. An agreement will also ensure clarity on enforcing citizens' rights.

Without an agreement which facilitates the free flow of data, there is a risk to:

- **Trade, consumers and public services**: It will be more difficult to protect consumer rights across borders, grow the data economy, and facilitate co-operation between public authorities without the free flow of data. All trade is increasingly reliant on data flows.

- **Citizens' security**: Swift and efficient exchange of personal data is essential in modern law enforcement to protect citizens and investigate serious crime and terrorism.

Trade, consumers and public services

Personal data flows are crucial to delivering the goods and services that citizens rely on in daily life. If data flows are disrupted, these **services are put at risk** across the economy, reflecting the **UK's and the EU's mutual interdependence** with regard to personal data flows.

RISKS IF FREE DATA FLOWS ARE DISRUPTED

Reduction in legal certainty and a rise in consumer scepticism, which could undermine trust in data protection frameworks and may put EU investments at risk.

EU and UK businesses struggle to put in place **costly alternative mechanisms** that may need time to set up e.g. a German based business utilising a UK Cloud provider for accounting information would have to find a new legal basis for the data-sharing, impacting their ability to do business efficiently

Vital public service **processes are disrupted** e.g. background checks, recognising qualifications.

VOLUME OF DATA FLOWS AT RISK

In the last ten years, global flows in goods, FDI and data have raised world GDP by more than 10%. **Data flows now account for a larger share of this growth than trade in goods**, contributing $2.8 trillion to the world economy.

It is estimated that the value of the European data economy could increase to €739 billion by 2020, representing **4% of overall EU GDP**.

EU exports to the UK of data reliant services were worth approximately **€36bn** in 2016. This includes a diverse range of sectors such as finance, telecoms and entertainment.

UK and EU citizens' security

The EU and UK need to continue to cooperate on the **secure and timely exchange of personal data** between law enforcement agencies to protect our citizens. Our Future Security Partnership will need to be **underpinned by agreed arrangements ensuring high standards of data protection.**

AREAS OF COOPERATION

Data-driven law enforcement and the swift and effective exchange of data between law enforcement agencies is critical to the co-operation needed to **tackle serious crime and terrorism.**

EU tools that allow for the **secure and timely exchange of personal data** depend on sharing alerts on wanted or missing persons to help bring criminals to justice and protect the most vulnerable; criminal records to ensure justice is delivered; and the sharing of passenger data to prevent and investigate serious crime and terrorism.

VOLUME OF COOPERATION

In 2016, the **UK responded to over 13,000 requests** for conviction information from EU Member States via ECRIS. In the same period, **the UK sent over 35,000 notifications to EU partners** regarding their nationals being convicted in the UK. This amounts to 9.3% of the overall notifications in Europe, making the **UK the fourth highest contributor**.

Between October 2015 and March 2017, the UK Financial Intelligence Unit (UKFIU) proactively disseminated **708 pieces of financial intelligence** to international financial intelligence units – 218 of which went to **Europol.**

Ambition to achieve high data protection standards globally

The EU and the UK both have an ambition to achieve high data protection standards on a global scale.

Building on our ground-breaking 1984 Data Protection Act, the UK has made a **significant contribution to the development of EU standards** - most recently the GDPR and Law Enforcement Directive.

The UK Information Commissioner's Office (ICO) and EU regulators work in close partnership and **exert influence in global fora**, such as the Global Privacy Enforcement Network and the International Conference of Data Protection Commissioners.

If our data protection authorities continue to work closely together, we will have **greater impact globally** to secure high standards of data protection.

The UK's data protection regime will be fully aligned with EU law

The UK is going beyond minimum EU requirements and will implement the GDPR and Law Enforcement Directive in full. Our Data Protection Act 2018 will provide a comprehensive and robust regulatory framework, compatible with the European Convention on Human Rights and Council of Europe Convention 108.

GENERAL DATA	The Act **extends** GDPR standards to cover general data outside the scope of EU law (e.g defence). The UK has made use of **permitted derogations** only, in full compliance with the GDPR.
LAW ENFORCEMENT DATA	The Act **incorporates** the Law Enforcement Directive (LED) into UK law. Although the LED only applies to the UK where data sharing is done under Title V police and judicial co-operation, the Act **extends** the LED to all processing (domestic and transnational) for law enforcement purposes.
NATIONAL SECURITY DATA PROCESSING	The Act provides a scheme for data processing for national security purposes, based on the draft modernised Council of Europe Convention 108. Separately, our national security legislation also incorporates high standards of privacy protection, transparency, accountability, safeguards and oversight.

UK implementation to prepare for the GDPR

The UK is undertaking a major programme to support effective and continued implementation of the GDPR by public authorities, businesses, and other organisations, **even the smallest businesses**.

> As a result of a targeted, awareness-raising campaign by the UK Government and the ICO, **77% of SMEs are aware of the new laws coming into effect on 25 May.**
>
> The ICO has produced and published a range of resources to help organisations prepare, supported by a **dedicated helpline** for smaller organisations**.** In particular, it has **produced detailed and developing guidance covering all aspects of GDPR**, including:
>
> - plain English "12-step" GDPR preparation guidance and adapted “8 step” version for micro businesses;
> - a range of toolkits to help compliance, including a specific SME version;
> - FAQs for a range of organisations and sectors (small local authorities, health sector bodies, and the education sector); and
> - GDPR ‘myth busting’ blogs.
>
> The ICO will continue to develop further guidance on the GDPR in light of Article 29 Working Group guidance. The UK Government has implemented a full governance system to ensure that the policies and systems it adopts continue to operate effectively under the GDPR.

The UK's proposals and the European Council Guidelines

The UK and the EU have both been clear on the importance of maintaining free flows of data.

UK Prime Minister, Mansion House, 2 March 2018	*Article 50 Guidelines, 23 March 2018*
"The free flow of data is also critical for both sides in any modern trading relationship too. The UK has exceptionally high standards of data protection. And we want to secure an agreement with the EU that provides the stability and confidence for EU and UK individuals and businesses to achieve our aims in maintaining and developing the UK's strong trading and economic links with the EU. "That is why we will be seeking an adequacy arrangement and ongoing regulatory cooperation through an appropriate ongoing role for the UK's Information Commissioner's Office. This will ensure UK businesses are effectively represented under the EU's new 'one stop shop' mechanism for resolving data protection disputes."	*"In the light of the importance of data flows in several components of the future relationship,* ***it should include rules on data.*** *As regards personal data, protection* ***should be governed by Union rules on adequacy*** *with a view to ensuring a level of protection essentially equivalent to that of the Union."*
UK Prime Minister, Munich, 17 February 2018	*Article 50 Guidelines, 23 March 2018*
"People across Europe are safer because of this [practical co-operation, data driven law enforcement and co-operation with EU agencies] co-operation and the unique arrangements we have developed between the UK and EU institutions in recent years."	*"The future partnership should cover* ***effective exchanges of information****, support for operational cooperation between law enforcement authorities and judicial cooperation in criminal matters."*

The standard adequacy approach

The standard adequacy approach is an effective means of ensuring a free flow of data from the EU to third countries. However, it would not reflect the breadth and depth of the UK-EU relationship.

> Adequacy Decisions allow the European Commission to recognise formally that a third country provides data protection standards that are **"essentially equivalent"** to those applied in the EU, and so personal data can flow freely without additional safeguards. Thus adequacy provides a legal basis that **enables the free flow of personal data** from the EU to a third country.
>
> The standard adequacy approach is informing the UK's approach to negotiations on the **Withdrawal Agreement**. It is important that the UK and the EU continue to protect the data and information exchanged before the end of the Implementation Period and on the basis of the Withdrawal Agreement to appropriate standards. The UK is willing to protect this data and information to a standard that is at least "essentially equivalent" to the level of protection in the EU at the end of the Implementation Period.
>
> The standard adequacy approach would not enable national data protection authorities to cooperate as effectively to enforce data protection principles. We therefore believe a **new model would better deliver both UK and EU interests**, and could provide more stability and certainty as an agreement between governments.

The greater benefits of a new agreement

The breadth and depth of the UK's relationship with EU partners, our full implementation of the EU framework and our shared ambition to achieve high data protection standards justify a new and innovative approach for our future partnership.

The UK therefore proposes a **new agreement** between the EU and UK, building on standard adequacy, that would better deliver on our shared interests. This would provide citizens in both the UK and EU with greater confidence in our data protection rules and standards.

Based on the following principles, it should:

- **maintain the free unhindered flow** of personal data between the EU and UK;
- offer **enhanced stability and confidence** for EU and UK individuals, businesses, and public authorities;
- **reassure** EU and UK citizens that their personal data is subject to robust protection;
- **not impose unnecessary additional costs** to EU and UK businesses; and
- provide for **ongoing regulatory co-operation** between the EU and the UK on current and future data protection issues, to ensure the framework effectively meets the needs of our unique relationship.

It could also provide clear processes for amendment, dispute resolution and termination.

How would a new model work?

The new agreement will build on a standard adequacy arrangement, reflecting the unique degree of convergence between the EU and the UK on data protection.

Key features of how we envisage the new agreement working.

- It will ensure **high standards of data protection** for personal data flows between the UK and the EU.
- It should provide for continued regulatory co-operation and consistent enforcement through an **appropriate ongoing role for the ICO on the European Data Protection Board**, to the benefit of consumers and businesses across the EU.
- It should ensure **UK businesses and consumers are effectively represented under the EU's new 'One Stop Shop'** mechanism for resolving data protection disputes when doing business in the EU. It will **benefit EU businesses operating in the UK to avoid two parallel processes** on data protection disputes - one in the UK led by the ICO and one in the 'One Stop Shop' and avoids unnecessary additional cost.
- It **could include amendment, dispute resolution and termination provisions.** This would provide EU and UK individuals and businesses with greater **stability** and **certainty**.

The Commission would conduct an **assessment** so as to assure itself that we meet the essential-equivalence test provided for in the GDPR and LED.

Contribution of the UK Information Commissioner's Office (ICO)

The ICO is the largest data protection authority in the EU, recognised by other European data protection authorities as a well resourced and highly valued centre of expertise, including internationally recognised work on AI and big data.

The ICO plays a leading and influential role in EU policy development, including as a member of the Article 29 Working Party (e.g. ICO was the lead or co-rapporteur for over 50% of the Working Party's work on guidelines in 2017). The ICO also plays a wider global role.

The ICO is an effective enforcer of EU rules, with a **strong record of independence** (e.g. investigation of its previous parent department, the UK Ministry of Justice).

WHY A CONTINUED ICO ROLE WILL BENEFIT UK AND EU CONSUMERS AND BUSINESS

- It will bring the ICO's **expertise, resource, experience and global influence** to bear.
- It ensures a **consistent approach** to interpretation and implementation of data protection principles.
- It **reduces the regulatory burden** on businesses with UK and European operations.
- It **helps EU consumers** bringing complaints against UK companies and **protects the rights of individuals**.

Conclusion

The UK is committed to a deep and special relationship with EU partners, in Europe and globally, to promote the free flow of data, underpinned by high data protection standards.

We seek a **new agreement on data protection**, that builds on a standard adequacy decision. Such a pragmatic approach would reflect our close shared interests and unique relationship, to the benefit of both the EU and UK.

A legally-binding agreement would:

- provide **strong privacy protections** for UK and EU citizens whose data flows between the UK and EU;
- underpin our **continued partnership**, notably on economic issues and security;
- provide **greater certainty** for consumers, businesses, law enforcement and other public authorities; and
- improve joined-up **regulatory enforcement** of data protection standards.