HM Government

The exchange and protection of personal data

A FUTURE PARTNERSHIP PAPER

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

This paper is part of a series setting out key issues which form part of the Government's vision for that partnership, and which will explore how the UK and the EU, working together, can make this a reality.

Each paper will reflect the engagement the Government has sought from external parties with expertise in these policy areas, and will draw on the very extensive work undertaken across Government since last year's referendum.

Taken together, these papers are an essential step towards building a new partnership to promote our shared interests and values.

The exchange and protection of personal data: a future partnership paper

Executive summary

1. Data flows are important for the UK and the EU economies and for wider cooperation, including on law enforcement matters. To ensure that individuals have control over and transparency as to how their personal data is being used, and that their personal data is protected from misappropriation and misuse, robust safeguards are needed.

2. The UK has strong domestic personal data protection standards, set out in the Data Protection Act (DPA) 1998. The UK's new Data Protection Bill, which will repeal and replace the DPA 1998, was announced in this year's Queen's Speech. It will further strengthen UK standards, ensuring they are up to date for the modern age, and it will implement the EU's new data protection framework in our domestic law. At the point of our exit from the EU, the UK's domestic data protection rules will be aligned with the EU data protection framework.

3. After leaving the EU, the UK will continue to play a leading global role in the development and promotion of appropriate data protection standards and cross-border data flows. In doing so we will work alongside the EU and other international partners to ensure that data protection standards are fit for purpose – both to protect the rights of individuals, but also to allow businesses and public authorities to offer effective services and protect the public.

4. After the UK leaves the EU, new arrangements to govern the continued free flow of personal data between the EU and the UK will be needed, as part of the new, deep and special partnership. The UK starts from an unprecedented point of alignment with the EU. In recognition of this, the UK wants to explore a UK-EU model for exchanging and protecting personal data, which could build on the existing adequacy model, by providing sufficient stability for businesses, public authorities and individuals, and enabling the UK's Information Commissioner's Office (ICO) and partner EU regulators to maintain effective regulatory cooperation and dialogue for the benefit of those living and working in the UK and the EU after the UK's withdrawal.

Introduction

5. The Commission has highlighted the value of the EU data economy, which was estimated to be worth €272 billion in 2015, or around two per cent of EU GDP. It has grown rapidly in recent years.[1] External estimates suggest that its value could rise to €643 billion by 2020, more than three per cent of GDP, as long as policy and legal frameworks for the data economy are put in place.[2]

[1] 'Building a European Data Economy', European Commission, January 2017.
[2] Ibid.

6. Increasingly, data flows envelop all trade in goods and services as well as other business and personal relations. The UK is a significant player in global data flows. Estimates suggest that around 43 per cent of all large EU digital companies are started in the UK[3], and that 75 per cent of the UK's cross-border data flows are with EU countries.[4] Analysis indicates that the UK has the largest internet economy as a percentage of GDP of all the G20 countries[5], and has an economy dominated by service sectors in which data and data flows are increasingly vital. The UK accounted for 11.5 per cent of global cross-border data flows in 2015, compared with 3.9 per cent of global GDP and 0.9 per cent of global population[6], but the value of data flows to the whole economy and the whole of society are greater still.

7. Any disruption in cross-border data flows would therefore be economically costly to both the UK and the EU. Taking EU-US data flows as a comparator, external estimates suggest that if cross-border data flows between the EU and the US were seriously disrupted, the EU's GDP could reduce by between 0.8 and 1.3 per cent.[7] Therefore, placing restrictions on cross-border data flows could harm both the economies of the countries implementing these policies, as well as others in the global economy.

8. Sharing personal data is also essential for wider cooperation that helps in the fight against serious crime and terrorism. The sharing of personal data is crucial to the EU's ongoing work across the continent to protect citizens, in which the UK plays an integral role. For example, between October 2014 and September 2015, the UK Financial Intelligence Unit (UKFIU) received 1,566 requests from international partners for financial intelligence. Of these, at least 800 came from EU Member States. In the same period, the UKFIU proactively disseminated 571 pieces of financial intelligence to international financial intelligence units, 200 of which went to Europol.[8] This intelligence contains personal data relating to individuals, companies and bank accounts suspected of connection with money laundering, terrorist financing and other financial crime. Well-designed, strong data protection standards go hand in hand with supporting innovative uses of data.

9. While personal data flows support both the UK and EU economies and the UK's wider cooperation with the EU, including on law enforcement matters, effective protections must be in place to ensure that data relating to individuals ('personal data') is handled appropriately and properly protected against any misuse, including when this data is transferred to another country.

---

[3] 'The Digital Economy', Business, Innovation and Skills Committee, House of Commons, July 2016.

[4] 'The UK digital sectors after Brexit', Frontier Economics, January 2017.

[5] 'The Internet Economy in the G20', Boston Consulting Group, March 2012.

[6] 'The UK digital sectors after Brexit', Frontier Economics, January 2017.

[7] 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce', European Centre for International Political Economy (ECIPE), March 2013.

[8] 'Suspicious Activity Reports (SARs) Annual Report 2015', National Crime Agency, March 2016.

Context

10. Recent technological advances have led to huge increases in the amount of personal data being processed and transferred, including across borders. Over time this has necessitated the development of more robust rules to:

    - protect personal data from being stolen or disclosed to those without authorisation;
    - prevent personal data from being misused by those who have access to it; and
    - keep personal data accurate, particularly where automatic decisions are being taken which have an impact on people, such as those concerning pensions, insurance, or creditworthiness.

11. In the UK, it has long been established that personal information should be protected in certain contexts. Doctors are expected to protect confidential information about their patients, and lawyers about their clients. Principles such as these existed long before any law dedicated to data protection was passed. The development of UK legislation on data protection can be traced back to at least 1970 and the establishment of the Younger Committee, and the UK's Data Protection Act 1984 was in place before the EU legislated in this area.

12. When the UK updated its data protection law to implement the EU Data Protection Directive 1995 (the 1995 Directive), it extended the rights and obligations beyond the minimum required by EU law. For example, the UK's update to the data protection law (DPA 1998) ensured that the same standards applied to certain types of law enforcement processing which were not covered by the 1995 Directive.

The EU data protection framework

13. The EU has recently updated its existing data protection framework (the 1995 Directive), in the form of a new General Data Protection Regulation (GDPR). This covers general processing of personal data within the scope of EU law, and a separate Data Protection Directive (DPD) relating to personal data being processed for law enforcement purposes. The UK played a full and active part in negotiations for the new GDPR and DPD, and the final text reflects a number of key UK priorities. For instance, the GDPR takes a more risk-based approach than had previously been adopted, with the result that certain obligations with which data controllers must comply are proportionate to the risk posed by the data processing activity. The GDPR and DPD were adopted in 2016 and are due to come into force in May 2018 (replacing the 1995 Directive), before the UK leaves the EU. The new rules strengthen rights and empower individuals by giving them more control over their personal data.[9]

14. The EU data protection framework includes mechanisms governing data flows between Member States and third countries.

    - All European Economic Area (EEA) states are directly party to the GDPR. For this reason, data can be transferred freely between EEA states without the need for businesses and public authorities to satisfy themselves in each case that the relevant national data protection safeguards are sufficient.

[9] 'Reform of EU data protection rules', European Commission, May 2016.

- For non-EEA countries, the EU data protection framework includes provisions allowing the Commission to decide that a third country's data protection framework is 'adequate', which allows data to flow freely between the EEA and those third countries. The existing adequacy model is discussed in paragraphs 32-41. Alternatives to adequacy are also available under the EU framework, but these can be more costly and onerous for businesses and public authorities, and are more limited in their application; Annex A sets out the alternatives to adequacy in more detail.

15. The GDPR will apply to processing of personal data that takes place in third countries outside of the EEA if it is related to the offering of goods or services to individuals in the EEA, or monitoring their behaviour. As such, UK businesses and public authorities may still be required to meet GDPR standards for their processing of EEA personal data following the date of withdrawal.[10]

16. The Government announced its plans in the Queen's Speech for a new UK Data Protection Bill which will replace the DPA 1998. This will ensure that the UK's framework is aligned with the updated EU legal framework at the date of withdrawal. The Government published its Statement of Intent on the Bill on 7 August 2017, setting out its proposed approach to the legislation in more detail.[11]

Other international data protection standards

17. The Council of Europe's Data Protection Convention (Convention 108) is a source of high-level data protection principles. It was signed in 1981 and is less detailed than the EU framework, which it pre-dates. Convention 108 is currently being modernised, in part to bring it more into line with the new EU data protection framework. Its high-level approach is likely to remain the same following completion of the modernisation process, although it is expected that there will be increased specificity in some provisions. The UK's data protection standards will remain fully aligned with the revised Convention 108.

18. Other international organisations have also noted the need for their own data protection principles. For example:

- the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted in 1980 and were updated in 2013 – they seek to harmonise national privacy legislation while preventing interruptions in international free flows of data; and

- the Asia Pacific Economic Forum Privacy Framework was adopted in 2005, recognising the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and support economic growth in the Asia Pacific region.

[10] See Article 3: Territorial Scope.
[11] 'A New Data Protection Bill: Our Planned Reforms', DCMS, 7 August 2017.

Outline of UK objectives

19. The UK recognises the need for, and is one of the leading drivers of, high data protection standards across the globe. An appropriate balance must be maintained between individuals' right to privacy and control over their own data, the ability of individuals, companies and other organisations to share data to create services which consumers value, and the ability of law enforcement bodies to protect citizens from crime and terrorism.

20. In an ever more connected world, we cannot expect data flows to remain confined within national borders. Moves towards data localisation, or the Balkanisation of the internet, risk stifling the competition, innovation and trade which produce better services for consumers, and can weaken data security. Global leadership and standards are needed to ensure that individuals can have confidence that their data is being appropriately protected wherever they choose to access goods or services, but not in such a way as to undermine the provision of those goods or services, including on a cross-border basis.

21. It is therefore the UK's ambition to remain a global leader on data protection, by promoting both the flow of data internationally and appropriate high levels of data protection rules. Case law demonstrates that there are divergent views globally on how to strike the right balance. The UK has played an important role in developing the EU's approach to data protection, including by playing a full part in the negotiation of the GDPR and DPD: throughout this process we promoted a balanced approach between freedoms and protections. The UK wants to continue to work closely with the EU, which has also been at the forefront of driving the improvement of global data protection standards, and our wider international partners, to work towards stronger global standards.

22. Underpinning this, as the UK and the EU build a new, deep and special partnership, it is essential that we agree a UK-EU model for exchanging and protecting personal data, that:

- maintains the free flow of personal data between the UK and the EU;
- offers sufficient stability and confidence for businesses, public authorities and individuals;
- provides for ongoing regulatory cooperation between the EU and the UK on current and future data protection issues, building on the positive opportunity of a partnership between global leaders on data protection;
- continues to protect the privacy of individuals;
- respects UK sovereignty, including the UK's ability to protect the security of its citizens and its ability to maintain and develop its position as a leader in data protection;
- does not impose unnecessary additional costs to business; and
- is based on objective consideration of evidence.

This could build on the existing adequacy model.

A UK-EU model for exchanging and protecting personal data between the UK and the EU, and beyond

23. A UK-EU model for exchanging and protecting personal data should recognise that the UK is compliant with EU data protection law and wider global data protection standards, and that the UK will introduce a Data Protection Bill which will, among other things, implement the GDPR and the DPD. In light of the UK's unprecedented position, the future deep and special partnership between the UK and the EU could productively build on the existing adequacy model (which is set out in more detail in paragraphs 32-41) in two key respects.

Regulatory co-operation

24. **After the UK's withdrawal, regulatory cooperation between the UK and the EU on a range of issues will be essential, including data protection** – not least because the GDPR will continue to apply to UK businesses offering goods or services to individuals in the EEA. A new relationship could therefore enable an ongoing role for the UK's ICO in EU regulatory fora, preserving existing, valuable regulatory cooperation and building a productive partnership to tackle future challenges.

25. The ICO works closely with other EU regulators and is well-regarded amongst its EU and international counterparts. Its resources and experience are a part of an established and effective EU regulatory dynamic. As the UK's data protection authority, the ICO plays an active role in helping determine the practical application of EU data protection law within EU fora.

26. A continued role for the ICO will support cross-border business and activity between the UK and the EU by promoting a common understanding of the regulatory challenges and issues faced by businesses, the public sector and individuals. The UK would be open to exploring a model which allows the ICO to be fully involved in future EU regulatory dialogue. An ongoing role for the ICO would allow the ICO to continue to share its resources and expertise with the network of EU Data Protection Authorities, and provide a practical contribution at EU level which will benefit citizens and organisations in both the UK and the EU. Indeed, this responds to the Commission's call to develop international co-operation mechanisms to facilitate effective cooperation and enforcement of data laws by data supervisory authorities.[12] The UK Government will continue to have responsibility for the content and direction of data protection policy and legislation within the United Kingdom.

Certainty and stability

27. In light of the existing alignment of our data protection frameworks, the UK also believes that a UK-EU model for exchanging and protecting personal data could provide an opportunity to give greater **ongoing certainty** to business and citizens in both the UK and the EU as to the rules governing future data flows, reducing the risks for business that the basis for data flows is unexpectedly changed.

---

[12] 'Exchanging and Protecting Personal Data in a Globalised World', European Commission, January 2017.

28. When the UK leaves the EU, it is essential that we avoid regulatory uncertainty for businesses and public authorities in the UK, EEA, and EU adequate countries who currently enjoy an ability to transfer data freely. Uncertainty over the nature of the data relationship between the UK and EU immediately on exit may force businesses on both sides to incur unnecessary expense and time in contingency planning, or put them under pressure to renegotiate what may be less favourable contractual arrangements. Ensuring certainty at the point of exit will avoid unnecessary disruption for businesses, public authorities and individuals in the UK and EU.

29. The UK's data protection law fully implements the EU framework, and this will remain the case at the point of our exit from the EU. On this basis, the Government believes it would be in the interest of both the UK and EU **to agree early in the process to mutually recognise each other's data protection frameworks** as a basis for the continued free flows of data between the EU (and other EU adequate countries) and the UK from the point of exit, until such time as new and more permanent arrangements come into force.

30. Early certainty around how we can extend current provisions, alongside **an agreed negotiating timeline for longer-term arrangements**, will assuage business concerns on both sides and should be possible given the current alignment of our data protection frameworks.

31. As well as ensuring that data flows between the UK and the EU can continue freely, the UK also wants to make sure that **flows of data between the UK and third countries with existing EU adequacy decisions can continue** on the same basis after the UK's withdrawal, given such transfers could conceivably include EU data. The UK is, and will remain after the point of withdrawal, a safe destination for personal data with some of the strongest domestic data protection standards in the world. For this reason, the UK does not see any reason for existing data flows from third countries to the UK to be interrupted. The UK will liaise with those third countries to ensure that existing arrangements will be transitioned over at the point of exit.

Existing EU processes and arrangements for international data flows

32. The 1995 Directive allows the Commission to formally recognise that a third country provides an 'adequate' level of data protection under EU law. Third countries do not formally agree or sign up to these decisions, although they are generally informed by prior discussions between the Commission and the third country regarding their domestic data protection law. Any areas where the Commission requires reassurance will require negotiation between the parties on how best to address the issues.

33. Adequacy decisions allow businesses and public authorities to continue to transfer data from the EEA to respective third countries without having to satisfy themselves that adequate safeguards are in place for each transfer.

34. Under current arrangements, any third country can request the Commission considers them for an adequacy decision. If it wishes, the Commission can then assess whether the nature of that country's data protection rules and the means for ensuring their effective supervision and enforcement, are sufficient to provide an adequate level of protection.

35. In making its assessment of a third country's data protection rules, the Commission will scrutinise that country's domestic legislation and practice, as well as compliance with relevant international standards, in order to ascertain whether the data protection standards in the third country are 'essentially equivalent' to those applied in the EU (a test set by the CJEU in Schrems).[13]

36. There is no set timeframe for the adequacy decision process. Once proposed, the decision needs to be confirmed by a panel of representatives from EU Member States, and the Commission can revoke the adequacy decision in the future. Adequacy decisions may also be invalidated by the CJEU.

37. To date, the Commission has adopted 12 adequacy decisions under the existing 1995 Directive, with: Andorra, Argentina, Canada (for transfers to commercial organisations who are subject to the Canadian Personal Information Protection and Electronic Documents (PIPED) Act), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the US (for certified companies). All are subject to routine review.

38. As well as adequacy decisions covering all transfers of personal data to a third country, partial adequacy decisions can be made covering only certain sectors of the economy. As mentioned above, two of the EU's current adequacy decisions are partial: the Canada Decision applies only to transfers of data to Canadian recipients who are subject to the PIPED Act; and the EU-US Privacy Shield is a different type of partial adequacy, in that it applies only to transfers to those companies in the US that have self-certified as having met the standards set out in the Privacy Shield framework. Various factors have, to date, been considered in determining whether to grant a partial or sector-specific adequacy decision (rather than a full decision), including whether there is an overarching data protection law in the third country, its constitutional structure and whether certain of its sectors are particularly exposed to data flows from the EU.

[13] Maxmillian Schrems v Data Protection Commissioner (C-362/14), Grand Chamber, 6 October 2015.

39. The new GDPR and DPD each contain adequacy provisions. Both measures amend some elements of the existing adequacy framework, providing a lot more detail on the elements the Commission must consider when coming to an adequacy decision. These include the rule of law, respect for human rights and fundamental freedoms, any international commitments entered into, and the third country's relevant legislation. The new framework also states that adequacy decisions should be reviewed periodically, and at least every four years.

40. On 10 January 2017, the Commission published a communication setting out its strategy for engaging selected third countries to reach adequacy decisions, starting with Japan and South Korea. It recently announced plans to conclude its adequacy decision with Japan by early 2018. This stems from a desire to achieve progress in the ongoing EU-Japan trade deal negotiations.

41. The new EU data protection framework also sets out a number of legal bases other than adequacy for transferring personal data to countries outside the EEA (see Annex A). Once the new framework has come into force, businesses and public authorities operating within and outside of the EEA will need to have one or more of these arrangements in place to underpin their transfers of personal data to non-EEA countries that do not have an EU adequacy decision. However, simply extending these provisions or establishing new ones to cover personal data transfers between the UK and the EU would be more burdensome for businesses and public authorities in both the UK and the EU, and would represent a missed opportunity to build a new partnership that reflects the close alignment of our data protection frameworks.

Conclusion

42. After leaving the EU, the UK will continue to play a leading global role in the development and promotion of appropriate data protection standards and cross-border data flows. In doing so we will work alongside the EU and other international partners to ensure that data protection standards are fit for purpose – both to protect the rights of individuals, but also to allow businesses and public authorities to offer effective services and protect the public.

43. Data flows between the UK and the EU are crucial for our shared economic prosperity and for wider cooperation, including on law enforcement. It is therefore essential that as part of the UK's future partnership with the EU, we agree arrangements that allow for free flows of data to continue, based on mutual trust in each other's high data protection standards.

44. Given that the UK will be compliant with EU data protection law and wider global data protection standards on exit, and given the important role of continued regulatory cooperation as part of a future economic relationship, the UK believes that a UK-EU model for exchanging and protecting personal data could provide for regulatory cooperation and ongoing certainty for businesses and public authorities. This could build on the existing adequacy model.

45. The UK's data protection law will fully implement the most up-to-date EU framework, and this will remain the case at the point of the UK's withdrawal from the EU. On this basis, the Government believes it would be in the interest of both the UK and EU to agree early in the process to mutually recognise each other's data protection frameworks as a basis for the continued free flows of data between the EU (and other EU adequate countries) and UK from the point of exit until such time as new and more permanent arrangements come into force.

46. As we leave the EU, the Government will also work with the devolved administrations and the governments of Gibraltar, the other Overseas Territories and the Crown Dependencies as we progress negotiations with the EU. We will continue to work closely with these governments on the detail of these proposals as they affect their interests.

Annex A: the alternatives to adequacy under the GDPR and DPD

1. Without an adequacy decision or new model in place, it is still possible for personal data to be transferred to third countries in some circumstances. In addition to various limited derogations from the general requirements, both the GDPR and the DPD set out alternative methods of transfer, which companies and public authorities may use to transfer data to third countries in the absence of an adequacy decision.

2. Under the GDPR, alternative legal bases for transfers of personal data outside the EEA include:

   - **Binding Corporate Rules** that allow the transfer of data between the establishments of a company located inside and outside the EU;

   - **Standard Contractual Clauses** that data controllers can adopt as the basis for data transfers; and

   - **Approved Codes of Conduct**, or approved certification mechanisms.

3. However, none of these alternatives are as wide ranging as an adequacy decision or an agreed new relationship. They can also be costly and onerous for businesses, especially for small and medium sized enterprises (SMEs).

   - Companies may need to pay for legal advice on what alternatives would be most appropriate.

   - Many companies may need their own customised contractual clauses drafted. These can be expensive and must be submitted for approval by EU regulators, which may take some time. Standard Contractual Clauses, as drafted by the Commission, do not require any approval but are inflexible and may not suit a particular company's processing situation.

   - Alternatively, businesses in the EEA wishing to transfer personal data to a UK branch could set up a Binding Corporate Rule. These also need approval by EU regulators and leading legal firms have indicated that on average they cost around £250,000 to set up.

   - Codes of conduct and certification mechanisms are insufficient by themselves: they must be accompanied by binding and enforcing commitments, which will entail legal costs, and must be approved by the European Data Protection Board.

4. Under the DPD, transfers to a third country or international organisation for law enforcement purposes are permitted in the absence of an adequacy decision. However, unless a derogation applies, this only applies where appropriate safeguards have been provided in a legally binding instrument, for instance, for a legally binding bilateral agreement between countries. Transfers can also occur in the absence of an adequacy decision where the controller has assessed all the circumstances and considers that appropriate safeguards exist.

5. Derogations for transfers in specific situations are also provided for in the DPD, but these are limited, for example, to protect the vital interests of the data subject or another person, or for the prevention of an immediate and serious threat to public security of a Member State or a third country. However, the ability to use these alternatives and derogations is more limited than adequacy.