DIGITALEUROPE

18 MAY 2021

EU-UK data transfers: a legal analysis supporting a swift adequacy decision

Introduction

The future relationship between the EU and the UK depends on the continued free flow of personal data, and securing adequacy for data transfers is of utmost importance to the future prospects of our economies. This paper provides an overview of why adequacy for the UK must be supported, in line with EU law and in light of the UK's solid data protection safeguards.

According to our latest survey,[1] six out of ten European businesses transfer data between the EU and the UK. These data flows contribute significant value to the economies and societies on both sides of the Channel, in terms of trade of both goods and services. EU personal data–enabled services exports to the UK were worth approximately €47 billion in 2018, and exports from the UK to the EU were worth €96 billion.[2] With a high proportion of trade in services, new business models of manufacturing industries enabled by data flows, the continued free flow of data between the EU and the UK is of crucial importance for the growth, digitisation and competitiveness of both EU and UK industries.

As a former Member State, the UK has helped build Europe's robust legal framework on data protection. The European Commission's draft adequacy decision[3] and the European Data Protection Board's (EDPB) Opinion on the decision[4] both find many core provisions of the UK data protection framework to be essentially equivalent to the GDPR.

---

[1] See DIGITALEUROPE, *Schrems II impact survey report*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

[2] Estimated by the UK government's Department for Digital, Culture, Media and Sport by applying the UN definition of digitally deliverable services to UK Office for National Statistics data.

[3] See draft Commission implementing decision on the adequate protection of personal data by the United Kingdom – General Data Protection Regulation, available at https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf.

[4] Opinion 14/2021, available at https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Despite finding a strong alignment between the EU and UK data protection regimes, the EDPB has raised a number of challenges to be further assessed and monitored by the European Commission. In this paper we address each of these challenges.

Table of contents

Divergence from EU data protection law

As clarified by the Court of Justice of the European Union (CJEU), and as stated in the European Commission's draft adequacy decision, the adequacy standard does not require a point-to-point replication of EU rules so long as long as the third-country rules 'prove, in practice, effective for ensuring an adequate level of protection.'[5] This includes ensuring that the UK's system as a whole delivers the required level of protection through assessing the effective implementation, supervision and enforcement of data protection rights.

The UK government has stressed its commitment to ensuring the UK maintains high standards of data protection, and that it will continue working with the Commission and other partners to promote strong data protection standards across the globe.[6] Any negative interpretation of the UK's interest in reforming its data protection regime is speculative and premature, and any future reform of UK data protection law should be scrutinised against the GDPR's adequacy requirements.

Safeguards under the UK immigration exemption

In 2019 the UK High Court ruled that the immigration exemption is lawful, and that the restriction 'is plainly a matter of "important public interest" and pursues a legitimate aim.'[7]

As found in the ruling, the immigration exemption is a high standard which, in common with the other exemptions provided for in the Data Protection Act 2018 (DPA), is not applied in a 'blanket way' but only on a case-by-case basis where it is necessary and proportionate to do so. In practice, this means that in the overwhelming majority of cases where the decision is taken to rely on the exemption, only a limited amount of data is restricted when responding to data subjects' access requests, and all other data is released to the data subject. On this basis, the exemption is never used to withhold anything that could assist an applicant's case.

---

[5] Para. 7, draft Commission implementing decision.

[6] See UK Minister for Media and Data, John Whittingdale MP, 'The UK's new, bold approach to international data transfers,' available at https://www.privacylaws.com/uk114data.

[7] Para. 30, Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor, available at https://www.bailii.org/ew/cases/EWHC/Admin/2019/2562.html.

The UK's Information Commissioner's Office (ICO) has issued guidance on the use of this specific restriction.[8] The guidance echoes that the immigration exemption should not be used to restrict rights for all the data being held and advises the controller to ensure the application of the exemption is proportionate to the circumstances and comply with the requirements of UK GDPR and the ICO as far as possible.

More specifically, the guidance sets out the rights of data subjects when the exemption is applied and that the exemption cannot be used to target any group of people, be they EU nationals or otherwise. The application of the exemption does not set aside all data subjects' rights, but only those expressly listed. UK authorities must be able to justify when they use the immigration exemption that there is a real risk of prejudice to effective immigration control.[9]

The use of the immigration exemption can be challenged. However the Home Office has not received any complaints on the use of the immigration exemption from the ICO since its introduction.

Under the European Union Settlement Scheme (EUSS), the UK has now issued settled status to over four million EU citizens, none of which have been adversely affected by the immigration exemption. The total number of applications concluded up to 31 March 2021 was 4,980,000.[10]

The Commission's draft decision clearly states that the immigration restriction, as interpreted by the case law and the ICO's guidance, is subject to a number of strict conditions which are 'very similar to the ones set in EU law for restrictions to data protection rights and obligations.'[11]

Furthermore, the Commission's draft decision notes the various avenues for redress in the event an individual believes their rights, including the right to privacy, have been infringed, notably through the Human Rights Act 1998 and the DPA. If national remedies are exhausted in the UK, individuals also then

---

[8] Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/immigration-exemption/.

[9] For example, data held on immigration databases may include information about planned and ongoing enforcement activities against those who are in the UK illegally. If, under an Art. 15 subject access request, the UK government were compelled to hand over such information to the subject of that enforcement activity, there is a real risk that the person will deliberately conceal their whereabouts.

[10] EU Settlement Scheme statistics, available at https://www.gov.uk/government/collections/eu-settlement-scheme-statistics.

[11] Para. 65, draft Commission implementing decision.

have the ability to refer their case to the European Court of Human Rights (ECHR).[12]

International commitments and onward transfers to other non-EEA jurisdictions

The UK's international data transfers regime

As of January 2021, the UK Secretary of State for Digital, Culture, Media and Sport (DCMS) can make adequacy decisions and adopt into UK law other transfer mechanisms enabling the overseas transfer of personal data, e.g. standard contractual clauses, consistent with the powers conferred to the European Commission under the GDPR.

As part of its comprehensive adequacy assessment, the Commission has reviewed the UK's international data transfers legislation and framework, finding the UK's regime on international transfers of personal data, set out in Arts 44-49 of the UK GDPR, to mirror that set out in Chapter V GDPR.

According to this regime, transfers of personal data to a third country or international organisation can only take place on the basis of 'adequacy regulations' or where the controller or processor has provided appropriate safeguards in accordance with Art. 46 of the UK GDPR. In the absence of adequacy regulations or appropriate safeguards, a transfer can only take place based on derogations set out in Art. 49 of the UK GDPR. Thus, when assessing the adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection 'essentially equivalent' to that guaranteed within the UK.

The procedure for adequacy regulations involves a number of checks and balances. Section 182 of the DPA 2018 stipulates that the Secretary of State must consult the ICO when proposing to adopt UK adequacy regulations, which are then laid before Parliament. The Memorandum of Understanding signed between the Secretary of State and the ICO sets out how they will maintain a close working-level engagement and share expertise in the context of future UK data adequacy decisions.[13]

---

[12] Section 2.6.4, ibid.

[13] See Memorandum of Understanding (MoU) on the role of the ICO in relation to new UK adequacy assessments, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971152/UK_Adequacy_Assessments__ICO-DCMS_Memorandum_of_Understanding_signed.pdf.

UK adequacy regulations must be reviewed at intervals of no more than four years. In case the Secretary of State becomes aware that a country or organisation no longer ensures an adequate level of protection, she must, to the extent necessary, amend or revoke the regulations and enter into consultations with the third country or international organisation concerned to remedy the lack of an adequate level of protection.

The UK government has stressed that it will continue to ensure that individuals' data protection rights are protected and upheld when their data is transferred overseas from the UK by considering the overall effect of a third country's data protection laws, implementation, enforcement and supervision. UK adequacy assessments will consider matters such as the rule of law, respect for human rights and fundamental freedoms, relevant legislation concerning public security, defence, national security and criminal law, and government access to personal data. Such assessments will also consider the international commitments into which the country has entered.

Onward transfers to the US through the UK-US agreement

Data transferred from the EU to service providers in the UK could be subject to orders for the production of electronic evidence issued by US law enforcement authorities and made applicable in the UK under the UK-US Agreement on Access to Electronic Data once in force.[14]

However, as noted by the Commission's draft decision, such agreement is subject to a number of safeguards. First, its material scope is limited to 'serious crimes,' including terrorist activity, that are punishable with a maximum term of imprisonment of at least three years. Moreover, data may be obtained only following an order by a court, judge, magistrate or other independent authority. Any order must 'be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation' and 'be targeted at specific accounts as well as identify a specific person, account, address, or personal device, or any other specific identifier.'[15]

Data obtained under this agreement also benefits from drafting that provides equivalent protections to those provided under the EU-US Umbrella Agreement,

[14] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

[15] Para. 152, draft Commission implementing decision.

which sets out the safeguards and rights applicable to data transfers in the area of law enforcement cooperation.[16] Data transferred to US authorities under the UK-US agreement should therefore benefit from an equal level of protection to that provided by an EU law instrument.

While the US-UK agreement was concluded in October 2019, it has not yet entered into force. The Commission's draft decision notes a commitment from the UK authorities to only let the agreement enter into force if there is clarity with respect to compliance with the data protection standards.[17]

Access by UK public authorities under national security and surveillance laws

The UK's data protection legislation provides independent oversight for the processing of personal data for law enforcement and national security purposes. The Investigatory Powers Act 2016 provides transparency and oversight over the use of investigatory powers in the UK. The processing of personal data by law enforcement agencies, as well as security and intelligence agencies, is governed by the below instruments which, together with the rest of the UK's framework, ensure the activities of the UK law enforcement, security and intelligence community adhere to strict principles of necessity and proportionality:

- Part 4 of the DPA, 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;
- The Investigatory Powers Act 2016 (IPA), which provides for transparency and oversight over the use of investigatory powers in the UK, and is overseen by the Investigatory Powers Commissioner, which publishes annual reports of its findings;
- Part 3 and Schedules 7-8 of the DPA, which together with provisions in Parts 5-7 apply across the UK GDPR's law enforcement and intelligence services regimes, transpose the provisions of the Law Enforcement

[16] Agreement between the United States of American and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.

[17] Para. 153, draft Commission implementing decision.

Directive (LED) into UK law.[18] This bespoke regime only applies to the processing of personal data by competent authorities for law enforcement purposes, and is tailored to the needs of the police, prosecutors and other law enforcement agencies. Like the UK GDPR and Part 4 of the DPA, 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 with, whilst enabling law enforcement officials to continue their important work. According to the Commission's draft decision, UK law imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes, and provides oversight and redress mechanisms in this area which are in line with EU law. In particular, Part 3 of the DPA sets out the principles of lawfulness and fairness, purpose limitation, data minimisation, accuracy, storage limitation and security.

Under the provisions of the IPA, the UK's intelligence agencies can only collect and access data where it is necessary and proportionate to do so. The UK does not practice mass surveillance. The collection of data by the UK intelligence agencies is subject to warrants approved by Ministers, and by specially appointed, independent judicial commissioners who must review the decision to issue a warrant applying judicial review principles.

The UK has on multiple occasions explained and clarified its national security data collection capabilities to the satisfaction of the ECHR. On the few occasions where minor failings have been found, these have been addressed. All UK intelligence agency staff that have access to data are required to undertake mandatory data protection and wider legalities training.

Bulk communications data powers are essential in helping identify subjects of interest, and in some cases may be the only investigative resource for intelligence agencies. Such powers has played an important part in every major counter terrorism investigation of the last decade. The CJEU has found that there are circumstances where Member States themselves can utilise such powers.[19]

There are strict safeguards governing UK access to data that has been collected in bulk. Before an analyst can select for examination any data obtained under a bulk warrant, they will need to ensure that it is necessary and proportionate for a specific operational purpose that will have been approved by the Secretary of State and a Judicial Commissioner at the point the warrant was issued.

The DPA allows for exemption from specified provisions where necessary to safeguard national security, but use of the exemption must be considered on a

[18] Directive (EU) 2016/680.

[19] C-623/17.

case-by-case basis. The exemption would permit the UK intelligence agencies, for example, not to confirm to a suspected terrorist that they are processing their personal data, where doing so would compromise national security by alerting them to the fact they are under surveillance. This is an established approach, consistent with Convention 108 and Protocols.[20] There are limited further exemptions, also subject to case-by-case consideration, for use in specific extenuating circumstances, such as to protect the armed forces.

The European Commission's draft decision states that through its membership of the Council of Europe, adherence to the European Convention of Human Rights and submission to ECHR jurisdiction, the UK is subject to a number of obligations enshrined in international law. These ensure its framework for government access to data is based on principles, safeguards and individual rights similar to those guaranteed under EU law.

The UK legal framework was recognised in 2018 by the UN Special Rapporteur for the Right to Privacy, Joseph Cannataci, as providing respect for individuals' right to privacy, transparency, safeguards, oversight and redress mechanisms.[21]

Procedural and enforcement mechanisms

The ICO is one of the largest data protection authorities in Europe, responsible for monitoring the application of the UK GDPR and processing by competent authorities for law enforcement purposes under Part 3 of the DPA. The ICO has a strong track record as an independent regulator capable of handling complex cases and imposing tough sanctions where necessary.

The Commission's draft decision finds that Art. 58 of the UK GDPR, setting out the ICO's powers, introduces no material changes to the corresponding GDPR provisions. Similarly, the EDPB acknowledged that the ICO's tasks and powers closely mirror those of its counterparts in the EU.

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.

---

[20] See *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence*, available at https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[21] See End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion of His Mission to the United Kingdom of Great Britain and Northern Ireland, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E.

Empowered to levy substantial administrative fines on organisations of up to £17.5 million or 4 per cent annual global turnover, the ICO has been one of the three active data protection authorities in recent years in terms of individual fining decisions. Between May 2018 and 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.[22]

In addition to complaints from data subjects, the ICO undertook over 2,000 investigations of potential civil and criminal infringements of data protection law in 2019-2020, issuing a number of fines and enforcement notices.[23]

Concerning exercising or investigative powers, the ICO has issued 65 information notices and 19 assessment notices since April 2018. This includes notices issued to six Political Parties, including the Conservative and Labour parties, as part of its investigation into political campaigning practices.

The ICO's supervision and action may involve a suite of outcomes ranging from advice, education, monitoring and audit.[24] For example, informal resolution may result in the ICO holding a data controller to account, resolving the complaint and binding the data controller to an improvement plan aimed at improving future compliance. This action may be followed up with an inspection. In terms of formal regulatory action, the ICO may exercise its corrective powers to address matters that present the greatest risk of harm to data subjects. Enforcement sanctions they have exercised include reprimands, enforcement notices and fines.

Further 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 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 is currently chair of

[22] See ICO website on enforcement action, available at https://ico.org.uk/action-weve-taken/enforcement/.

[23] The ICO issued a fine of £275,000 to Doorstep Dispensaree for failing to secure sensitive personal data, ensure appropriate organisational security measures and for failing to provide data subjects with information about processing. This was accompanied by an enforcement notice requiring them to improve their practices. The ICO has also issued fines to British Airways, Marriott International, Inc. and Ticketmaster of £20 million, £18.4 million and £1.25 million, respectively, for data security breaches via the Art. 60 process. The ICO has issued 20 Enforcement Notices since May 2018 to HMRC for unfair and unlawful collection of voice biometrics for people calling their helpline.

[24] See ICO Regulatory Action Policy, available at https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

the Global Privacy Assembly. The ICO also has experience working closely with other data protection authorities. The ICO was the lead or co-rapporteur for many of the Article 29 Working Party guidelines, and the lead authority on dozens of cases before the UK left the EU. Many other data protection authorities have re-used the ICO's domestic guidance. Moreover, with approximately 750 staff, the ICO is well resourced, enabling it to develop expertise in niche areas such as the impact of new technologies on privacy rights, increasing its ability to take effective enforcement action.

Conclusion

This paper has highlighted the comprehensive safeguards enshrined in the UK legal framework, building on the challenges raised by the EDPB. These safeguards are consistent with the *Schrems II* requirements,[25] including for government access, and all support a positive adequacy finding.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Manager

martin.bell@digitaleurope.org / +32 492 58 12 80

[25] See paras 113-115, draft Commission implementing decision.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, TECH IN France
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK