Title: The Post-Brexit Need for a Data Adequacy Decision to Engage in Mutual Assistance in Criminal Matters with the EU

Author(s): Matthew G T Bruce


Published by: Institute of Legal and Constitutional Research, University of St Andrews

Stable URL: https://doi.org/10.15664/stalj.v3i1.2646

DOI: 10.15664/stalj.v3i1.2646

This work is protected under Creative Commons Attribution 4.0 International (CC BY 4.0) License 2020.

The author(s) retain copyright holding, having permitted the University of St Andrews Law Journal to distribute (publish) their work.

The University of St Andrews Law Journal is an Open-Access publication of the University of St Andrews, recorded by the ISSN National Centre for the UK. Published in partnership with the Institute of Legal and Constitutional Research, University of St Andrews.

Copyright @ 2023 University of St Andrews Law Journal

All use subject to:
https://creativecommons.org/licenses/by/4.0/

ISSN 2634-5102
THE POST-BREXIT NEED FOR A DATA ADEQUACY DECISION TO ENGAGE IN MUTUAL ASSISTANCE IN CRIMINAL MATTERS WITH THE EU

by Matthew G T Bruce

Mutual assistance and data protection laws as they apply to member states

Mutual assistance in criminal matters between EU member states is primarily governed by an EU convention.¹ This convention builds on existing Council of Europe (CoE) conventions on mutual criminal assistance.² The EU convention states that mutual assistance shall be afforded in proceedings brought by member states’ authorities, or in connection with proceedings where a person may be liable in the requesting member state.³ Title II provides a framework for specific forms of assistance including restitution, hearings via videoconference and covert investigations.⁴ Member states are free to conclude further bilateral arrangements.⁵

While a member state, the UK’s data protection laws, including in the area of criminal cooperation, originated from the EU. Law enforcement data protection law is set out in Directive 2016/680 (LED).⁶ The LED was incorporated into domestic UK law by Part 3 of the Data Protection Act 2018. It is not as stringent as the General Data Protection Regulation (GDPR),⁷ regarding commercial and personal data, and affords member states a margin of appreciation when implementing its provisions domestically.⁸ The LED only applies when member states are acting within the scope of EU law.⁹ Member states’ national security agencies are not subject to

---

² CMA, art 1(1)(a).
³ CMA, art 3.
⁴ CMA, Title II.
⁵ CMA, art 22.
⁹ LED, art 2(3)(a).
EU law as they remain in the post-Lisbon Area of Freedom, Security and Justice. The LED does not apply to EU agencies either. EU agencies which deal with criminal matters, such as Europol, are subject to their own data protection regimes. The Europol Regulation is arguably stricter than the LED regrading data protection. The LED, therefore, allows for member states to operate at a lower data protection level than they would if they cooperated solely through Europol. When implemented domestically, the rights of data subjects do not apply during criminal investigations and proceedings. The provisions apply to UK law enforcement when operating cross-border with other states. It is argued that this implementation worked well with UK Government policy when cooperating in mutual assistance in criminal matters pre-Brexit.

An area in which there is a significant legal framework regarding the transfer of data is for passenger name records (PNR). The PNR Directive sets out provisions for harmonisation of law relating to the receiving, processing and sharing of PNR data for law enforcement and security purposes. The main purpose of the PNR Directive is for extra-EU flights, but member states can apply its provisions for all or selected intra-EU flights. The PNR Directive requires compliance with the LED when transferring data to third countries.

The PNR Directive sets out that member states should have regard to relevant Court of Justice of the European Union (CJEU) decisions regarding privacy, proportionality and fundamental rights. The CJEU does apply such law stringently to the EU’s PNR and data adequacy.

---

11 LED, art 2(3)(b).
13 Cocq (n 9), 266.
14 Ibid., 275.
15 Data Protection Act 1998 (DPA 1998), s 43(3); LED, recital (20); Caruna (n 11), 259.
16 DPA 2018, s 72; LED, recital (74); Caruna (n 11), 252.
arrangements.\textsuperscript{24} Van de Heyning concludes that the CJEU takes a stricter view than other EU institutions when assessing member states' application of data protection law in criminal matters.\textsuperscript{25}

**Law underpinning data adequacy decisions**

Adequacy decisions are made by the European Commission to allow for the transfer of data between the EU and a third country.\textsuperscript{26} They are not unique to post-Brexit Britain. The Commission has granted decisions to a number of third countries.\textsuperscript{27} The UK is unique in that it has been received two separate decisions under the GDPR\textsuperscript{28} and LED.\textsuperscript{29} The purpose of decisions is to show that there is an equivalence of data protection laws between the EU and a third country.\textsuperscript{30} The UK is not treated differently having previously been a member state, although domestic data protection laws implement the most recent EU legislation.\textsuperscript{31}

Decisions are not long-term guarantees of the free movement of data. The LED decision is valid for a period of four years, after which it must be reassessed and reissued by the Commission.\textsuperscript{32} By granting an adequacy decision, the Commission has assessed, \textit{inter alia}, the UK’s: legislation concerning public and national security;\textsuperscript{33} law pertaining to the onward transfer of data to other third countries and international organisations;\textsuperscript{34} independent supervisory authorities;\textsuperscript{35} and, legally binding commitments.\textsuperscript{36}

There is no guarantee of the longevity of decisions. The seminal case of \textit{Schrems} made this clear.\textsuperscript{37} There are three main elements of the CJEU’s judgement in this case. First, that member

\begin{footnotesize}
\textsuperscript{24} Opinion 1/15 of the Court (Grand Chamber) [2017] ECLI:EU:C:2017:592.
\textsuperscript{25} Catherine Van de Heyning, 'Data protection and passenger name record in judicial criminal matters under the EU-UK Trade and Cooperation Agreement' (2021) 12(2) New Journal of European Criminal Law 257, 264.
\textsuperscript{26} GDPR, art 45; LED, art 36.
\textsuperscript{30} n 36-49.
\textsuperscript{32} LED, art 36(3).
\textsuperscript{33} LED, art 36(3)(a).
\textsuperscript{34} LED, art 36(3)(b).
\textsuperscript{35} Ibid.
\textsuperscript{36} Ibid, art 36(3)(c).
\textsuperscript{37} Case C-362/14 \textit{Schrems v Data Protection Commissioner} [2015] ECR-I 00000.
\end{footnotesize}
states’ national supervisory bodies, not just the Commission, are able to investigate a third
country’s data adequacy.\textsuperscript{38} Second, that the handling of data by a third country’s national
security agencies, of which member states’ are not within the competence of the EU,\textsuperscript{39} is subject
to the EU’s adequacy requirements.\textsuperscript{40} Third, the CJEU is able to strike out an adequacy decision
if it finds that a third country is not providing adequate data protection.\textsuperscript{41} Schrems also made
clear that ‘adequate data protection laws’ mean laws that are ‘essentially equivalent’ to those of
the EU.\textsuperscript{42} The same applied to adequate protection of PNR data in third countries, with a
decision granted to Canada annulled.\textsuperscript{43}

EU case law has developed strict rules relating to data protection. The CJEU has held that it is
incompatible with the Charter of Fundamental Rights of the European Union (CFREU)\textsuperscript{44} for
telecommunications companies to be under a general and indiscriminate obligation to retain
communications data,\textsuperscript{45} due to the precise conclusions that can be drawn from it.\textsuperscript{46} Derogations
are allowable if the retention is necessary, appropriate and proportionate in a democratic
society.\textsuperscript{47} In Privacy International,\textsuperscript{48} the Court held that the Charter precludes an obligation on
companies carrying out an indiscriminate transmission of data to security and intelligence
agencies.\textsuperscript{49} Most recently Schrems II makes alternatives to adequacy decisions, such as standard
contractual clauses, more difficult to maintain.\textsuperscript{50} These must still be adequate in relation to EU
law.\textsuperscript{51} This case dealt with the transfer of commercial data but is provides guidance on how the
CJEU could act in response to litigation regarding LED decisions.\textsuperscript{52}

The CJEU’s rulings have been described as a ‘bridle’ over the UK.\textsuperscript{53} The UK must maintain
equivalence to EU law to maintain its adequacy decision while carefully monitoring all aspects of
its domestic data protection laws and obligations.\textsuperscript{54} Although the LED adequacy decision relates

\textsuperscript{38} Schrems (n 38), [51]-[52].
\textsuperscript{39} n 11.
\textsuperscript{40} Schrems (n 38), [25].
\textsuperscript{41} Schrems (n 38), [106].
\textsuperscript{42} Schrems (n 38), [73].
\textsuperscript{45} Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2017] 2 CMLR 30, [92]; Case C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources [2014] 3 CMLR 44.
\textsuperscript{46} Tele2 (n 46), [99].
\textsuperscript{47} Tele2 (n 46), [95].
\textsuperscript{48} Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs [2020] ECR-I 00000.
\textsuperscript{49} Privacy International (n 49), [50].
\textsuperscript{50} Case C-311/17 Data Protection Commissioner v Facebook Ireland Ltd [2021] 1 CMLR 14 (Schrems II).
\textsuperscript{51} Schrems II, [H4].
\textsuperscript{52} Lorna Woods, ‘Schrems II’ (2020) 25(4) Communications Law 239.
\textsuperscript{53} Celeste (n 32), 9.
\textsuperscript{54} Ibid.
specifically to the transfer of data in criminal matters, it is not just the domestic UK data protection laws relating to criminal matters that are under observation by the EU. Constitutional arrangements such as the rule of law;\textsuperscript{55} respect for human rights and the independence of supervisory bodies;\textsuperscript{56} and international commitments of the UK will be under EU observation.\textsuperscript{57} With all of these aspects under constant review there is the risk that if one fails in the courts, it could nullify the entire the LED data adequacy decision.\textsuperscript{58}

The European Parliament has made clear that the UK should be cautious when developing its domestic law to avoid the same result as the Schrems cases: recognising this result will be detrimental for mutual assistance.\textsuperscript{59} It is argued that that the investigatory powers of EU institutions removes certainty from decisions issued.\textsuperscript{60} Case law in this area allows for NGOs and the public to be disruptive through litigation.\textsuperscript{61} Therefore, the only feasible way to maintain an adequacy decision is to keep closely aligned to EU law and principles.\textsuperscript{62}

**Adequacy decisions and future legal development in post-Brexit Britain**

As of now, the data protection law in the UK is deemed equivalent to the EU’s. However, the legal relationship between the UK and EU has changed post-Brexit and consequences of divergence may be more significant than would be for an EU member state. While a member state, certain aspects of member states’ institutions, notably their security services, are outside the scope of EU law with a degree of flexibility for the UK when determining data protection in these areas. Though not referred to in the LED, the actions of national security agencies will now be observed to comply with data protection law.\textsuperscript{63} In the UK, Part 4 of the 2018 Act sets out six principles that must be observed when processing data related to national security:\textsuperscript{64} data processing must be lawful, fair and transparent; for a legitimate purpose; relevant; kept up to

\textsuperscript{55} LED, art 36(2)(a).

\textsuperscript{56} Ibid.

\textsuperscript{57} LED, art 36(2)(c).

\textsuperscript{58} Andrew D Murray, ‘Data transfers between the EU and UK post-Brexit’ (2017) 7(3) International Data Privacy Law 149.


\textsuperscript{60} Theodore Christakis, ‘EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options’ (2021) 11(2) International Data Privacy Law 81.

\textsuperscript{61} Ibid.


\textsuperscript{63} Schrems (n 38).

\textsuperscript{64} DPA 2018, ss 86–91.

Copyright © The Author(s)
Part 4 may have sufficed while the UK was a member state, however, to maintain equivalence with EU law as a third state the UK must have regard and implement decisions of the CJEU. These go much farther in setting out protections.

A notable difference between the UK and other third countries is the TCA, which contains provisions on cooperation in criminal matters including PNR, the exchange of criminal record information and relations with Europol. The TCA sets out that data protection is subject to each party’s legal framework. It provides the principles which data protection should be based on rather than a specific means of doing so. Each separate title on cooperation must be considered individually to assess the framework of data protection required.

The TCA sets limits on the use of PNR data; ensures its free movement from the EU and obliges the UK to ensure its security. It is suggested that for operation of the TCA’s PNR provisions there must be an adequacy decision in place, based on the EU framework for PNR data referring to compliance with the LED for transfers to third countries. The TCA PNR provisions place the UK in a strong position as a third country. The same is true for the transfer of criminal record information, with conditions in place for the transfer of requested information. This title is intended to supplement Council of Europe conventions on mutual assistance in criminal matters. The Europol title details that the sharing and storage of data between Europol and UK competent authorities should be dealt with under the respective parties’ domestic legal frameworks. None of these titles make reference to the specific need for an adequacy decision to enable their operation. Cooperation under the TCA is less detailed than it is for member states, but high standards of data protection are built in which may, in practice, be conditional for the operation of the TCA.

---

65 LED, recital (3).
66 TCA, art 525(2).
67 TCA, art 525(2)(a)-(h).
68 TCA, art 544 and annex 40.
69 TCA, art 545(1).
70 TCA, art 549.
71 Van de Heyning (n 26).
74 TCA, arts 643 – 651; TCA, annex 44.
75 TCA, art 651.
76 TCA, arts 643(2)(a) – (b).
77 TCA, art 570(3).
Should the UK adequacy decision be nullified by the CJEU, it would automatically halt the free movement of data for criminal matters between the EU and the UK. Nevertheless, there are provisions built into the LED which still allow for the transfer of data in criminal matters between member states and third countries. If, in the UK, there are appropriate safeguards in a legally binding instrument, or the data controller deems such safeguards to exist, data may be transferred to a third country. If there are no safeguards and no adequacy decision, data may be transferred if: it protects the vital interests of a person; safeguards the legitimate interests of the data subject; prevents an immediate threat to the public; or for the prevention, investigation, detection or prosecution of a crime. However, in the event the adequacy decision is nullified, these provisions may be difficult to exercise if there has been any significant change in UK law.

The UK is no longer party to the EU convention on mutual assistance. It is, however, still party to the CoE convention on mutual assistance. This is not as extensive as the EU convention, but it does oblige contracting parties to ‘undertake to afford’ mutual assistance when requested. The CoE convention does not contain provisions on specific assistance and is not binding on contracting parties in the same way as EU law. The UK could request mutual cooperation in a bilateral or multilateral manner on the basis of this convention.

As is clear from the above analysis, the UK government’s future policy decisions could have a detrimental effect on the LED adequacy decision, or the renewal of any future decision. The UK Government has recently concluded a deal with Amazon Web Services to hold intelligence data of three UK intelligence agencies, GCHQ, MI5 and MI6. This, and the Five Eyes intelligence alliance, are aspects of domestic UK policy that may negatively affect the longevity of the LED decision. While most UK law is now outside the jurisdiction of the CJEU and CFREU, the European Court of Human Rights is developing data protection law which the UK is still bound

79 LED, art 37.
80 LED, art 38(1)(a).
81 LED, art 38(1)(b).
82 LED, art 38(1)(c).
83 LED, arts 38(1)(e) and 1(1).
85 ECMA, art 1(1); Davidson (n 18), 385.
88 Celeste (n 32).
Strasbourg jurisprudence may act as an equivalence between the UK and the EU, provided the UK follows its judgements.

**Conclusions**

There is overwhelming consensus that an adequacy decision concluded under article 36 of the LED is needed to maintain positive and efficient mutual assistance between the UK and EU in criminal matters. However, it is not the only way of achieving this aim. The law relevant to adequacy decisions has undergone significant litigation in the CJEU, resulting in strict data protection requirements which must be met by third countries. The current legal framework underpinning adequacy decisions and mutual assistance with third countries could be self-limiting for the EU’s own interests. By creating a much stricter framework for third countries, it is becoming increasingly more difficult to maintain adequacy decisions. Therefore, the EU must balance its own need for mutual assistance with the UK while upholding EU data protection principles.

The TCA puts the UK in a unique position amongst third countries. None of its provisions mention the need for a data adequacy decision for their operation. While not being as efficient and detailed as intra-EU provisions, this demonstrates that for the UK there are a number of options available. While the TCA may be a sufficient fallback in the absence of an adequacy decision, its titles too could face restriction or unilateral suspension depending on UK conduct in the area of data protection. The TCA’s provisions are not isolated from EU law either; the UK may still need to maintain equivalence with the EU, such as compliance with the CJEU as

---

90 Irena Ilc, ‘Post-Brexit limitations to government surveillance: does the UK get a free hand?’ (2020) 25(1) Communications Law 31; Big Brother Watch v United Kingdom (58170/13, 62322/14, 24969/15) [2021] 5 WLUK 463.
91 Ilc (n 91).
93 Laura Drescher, ‘Wanted: LED adequacy decisions. How the absence of any LED adequacy decision is hurting the protection of fundamental rights in a law enforcement context’ (2021) 11(2) International Data Privacy Law 182.
94 Ibid.
96 TCA, Title XIII and art 700; Wolfgang Shomburg, Anna Oehmichen and Katrin Kayß, ‘Human rights and the rule of law in judicial cooperation in criminal matters under the EU-UK Trade and Cooperation Agreement’ (2021) 12(2) New Journal of European Criminal Law 246.

Copyright © The Author(s) CC BY 4.0
detailed in the PNR Directive,\textsuperscript{98} for TCA provisions to operate effectively.\textsuperscript{99} EU member states and institutions are still bound by EU law; much of which does make reference to adequacy decisions under the LED as the preferred option for cooperation in criminal matters with third countries.

This analysis shows that there are several options available to maintain cooperation in criminal matters. However, the LED adequacy decision provides the most efficient method of achieving this: despite its vulnerabilities. There are other routes available under the TCA and LED but without an adequacy decision in place these too could face difficulties or suspension. There is, therefore, a need for a data adequacy decision to maintain efficient mutual assistance in criminal matters.

\textsuperscript{98} n 22-24.
\textsuperscript{99} Engel (n 98).
BIBLIOGRAPHY

Treaties

European Union


Trade and Cooperation Agreement between the European Union and European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [2021] OJ L149/10; implemented by European Union (Future Relationship) Act 2020

Council of Europe


Legislation

European Union

Regulations


Directives

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of
criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L127/18


Resolutions

European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18 (2020/2789 (RSP))

Parliament of the United Kingdom

Data Protection Act 1998 (c 12)

European Union (Future Relationship) Act 2020 (c 29)

Adequacy Decisions


Cases

European Union

Data Protection Commissioner v Facebook Ireland Ltd (Case C-311/17) [2021] 1 CMLR 14

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (Case C-293/12) [2014] 3 CMLR 44

Opinion 1/15 of the Court (Grand Chamber) [2017] ECLI:EU:C:2017:592

Privacy International v Secretary of State for Foreign and Commonwealth Affairs (Case C-623/17) [2020] ECR-I 00000

Schrems v Data Protection Commissioner (Case C-362/14) [2015] ECR-I 00000

Tele2 Sverige (Joined Cases C-203/15 and C-698/15) [2017] 2 CMLR 30

United Kingdom

Big Brother Watch v United Kingdom (58170/13, 62322/14, 24969/15) [2021] 5 WLUK 463


European Court of Human Rights

Secondary Articles


Christakis T, ‘EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options’ (2021) 11(2) International Data Privacy Law 81


Ilc I, ‘Post-Brexit limitations to government surveillance: does the UK get a free hand?’ (2020) 25(1) Communications Law 31


Murray A D, ‘Data transfers between the EU and UK post-Brexit’ (2017) 7(3) International Data Privacy Law 149


Websites


Van de Heyning C, ‘Data protection and passenger name record in judicial criminal matters under the EU-UK Trade and Cooperation Agreement’ (2021) 12(2) New Journal of European Criminal Law 257

