Commercial Data Transfers and Liaison Officers: What Data Protection Rules Apply in the Fight against Impunity When Third Countries Are Involved?

Eckes, C.; Barnhoorn, D.

DOI
10.2139/ssrn.3493611
10.5040/9781509926909.ch-017

Publication date
2020

Document Version
Final published version

Published in
The Fight Against Impunity in EU Law

17

Commercial Data Transfers and Liaison Officers: What Data Protection Rules Apply in the Fight against Impunity When Third Countries Are Involved?

CHRISTINA ECKES AND DOMINIQUE BARNHOORN

I. Introduction

Data protection is one of the great challenges of the twenty-first century. More and more data is stored, transferred, sold and analysed. It is used to enforce the law and to influence public opinion, including elections and referenda.[1] Once data leaves the jurisdiction of the European Union, it is accepted that the data protection rules are different and that the level of protection is lower than within the EU legal order. Nonetheless, large quantities of personal data leave EU territory every day as part of routinised commercial interaction. In addition, the EU invites seconded civil servants from third countries, who do not fall within the jurisdiction of the EU, cannot be held accountable in the same way and do not answer to the same rules, to work in its agencies and have access to data.

This chapter addresses the question of whether and under what circumstances data protection should prevail over the fight against impunity. It focuses on data cooperation between the EU and the USA in the context of crime prevention and law enforcement. It examines the limited control mechanisms that are in place to ensure data protection after data has been transferred or otherwise shared in the highly relevant and controversial context of commercial transfers of personal data and in the academically rather neglected context of liaison officers seconded from the USA to EU agencies within the area of freedom, security and justice (AFSJ).

[1] On the latter point, see: https://www.theguardian.com/news/series/cambridge-analytica-files. On the latter point, see www.theguardian.com/news/series/cambridge-analytica-files. On the latter point, see www.theguardian.com/news/series/cambridge-analytica-files.

The objective is to identify limits imposed by data protection requirements on data sharing as a means of fighting impunity, responsibilities of EU actors for data that is collected and processed within the EU's jurisdiction, be it public or private actors, and limits of the EU's control over data flows in the twenty-first century.

The paper is structured as follows. Section II briefly sketches the EU's legal framework for data protection. Section III turns to transfers of personal data in the context of commercial transactions and national security. It engages with the Court of Justice of the European Union (CJEU)'s recent case law on data protection, including the cases of *Schrems I* and *Schrems III*, which specifically concern the rules and guarantees that apply to commercial data transfers. National security exemptions in the EU data protection framework are examined and it is explained why they cannot apply to data transfers to third countries. This makes it very difficult to determine what standard of protection must apply in the third country for the data transfer to be legal under EU law. EU secondary law also does not require the same or even an equivalent level of protection. The section concludes with the checks and balances within the EU's data protection framework, and reflects on whether a differentiated approach toward data transfers between the EU and third countries is desirable. Section IV focuses on the specific example of data transfers via liaison officers in the AFSJ. Liaison officers are introduced as intermediate actors between two administrations – in this case, Europol and the US administration. It examines whether and how EU data protection standards could apply to liaison officers deployed from the USA to Europol. Section V then argues that protection of data that leaves the jurisdiction of the EU cannot be guaranteed at the same level as data within the jurisdiction of the EU. Similarly, when seconded civil servants of third countries are given access to data within the EU institutions, agencies and bodies, they are not subject to the same data protection rules as the EU's or Member States' civil servants. Ultimately, the two cases of commercial data transfers and the deployment of liaison officers demonstrate that data cooperation always comes at some cost in terms of data protection.

II. EU Data Protection Framework

Data protection is guaranteed within the European Union as a fundamental right in Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights (CFR). The right's personal scope is 'everyone'. In addition, Article 16 TFEU serves as a specific legal basis for adopting legislation to give effect to this right. The main secondary pieces of legislation are the 2016 General Data Protection Regulation (GDPR) and the 2016 Directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes.[2]

[2] Regulation (EU) 2016/679 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 and on the free movement

In May 2018, the GDPR replaced the previously applicable Data Protection Directive of 1995 (DPD)[3] for (inter alia) the specific issue of transferring personal data to third countries. In relation to data transfer to third countries, Article 45 GDPR replaced Article 25 DPD. Both provisions require an 'adequate' level of protection.[4] The Commission adopts general 'adequacy decisions' that address the general level of protection within the third country.[5] The Data Protection Authorities (DPAs) examine specific requests from individuals. 'Adequacy' implies that the standard does not have to be the same but that in fact data transfer is legal when a different, lower standard applies after the data has left the jurisdiction of the EU.

In 2016, the EU concluded an umbrella agreement with the USA on data transfers to the USA for law enforcement purposes. The EU placed a number of demands on the USA for the agreement to be concluded, such as that the US Judicial Redress Act extends the protection of the US Privacy Act of 1974 to EU citizens.[6] In addition, the USA also adopted the US Freedom Act 2015. However, it is fairly uncontroversial that domestic legal rules in the USA and international commitments do not guarantee a level of protection equivalent to the protection in the EU. They do not exclude access to personal data on a generalised basis, which was specifically found to be illegal under EU law (*Digital Rights Ireland*),[7] and which also interferes with the core of the right to private life as it is protected under the CFR and the European Convention of Human Rights (ECHR). In terms of remedies provided, the USA does not offer the full scope required under EU law (possibility to judicially enforce access, rectification and erasure).[8]

Within the EU legal order, international agreements rank between primary and secondary law. This means, in principle, that international commitments cannot be reviewed in the light of secondary law and that secondary law is interpreted in line with international agreements (consistent interpretation). Exceptions to this general hierarchy can be argued on the basis of the CJEU's line of case law of *Mangold* and *Kücükdeveci*,[9] where secondary law gives specific expression to a

of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR); 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 L119/89.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[4] Art 25(1) DPD; Art 45(1) GDPR.

[5] Art 25(6) DPD; Art 45(1) GDPR; see also recitals 103–07 GDPR, emphasising the Commission's role and the EU's commitment to fundamental rights.

[6] Judicial Redress Act of 2015.

[7] Joined Cases C-29312 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* ECLI:EU:C:2014:238.

[8] Art 8 CFR.

[9] Case C-144/04 *Werner Mangold v Rüdiger Helm* ECLI:EU:C:2005:709; Case C-555/07 *Seda Kücükdeveci v Swedex GmbH & Co KG* ECLI:EU:C:2010:21.

general principle of EU law or a fundamental right protected under the Charter.[10] In these exceptional cases, secondary law is in fact understood as a concretisation of the general principle or right under primary law and as such can influence the interpretation and validity of international agreements. In the present context, one could imagine that certain core principles of the GDPR could be considered an expression of the general right to protection of personal data. This would exclude that international agreements with the USA could disregard the protection provided under the GDPR.

If this were not the case, however, the general hierarchy (international agreements rank between primary and secondary law) means that, in principle, the executive could, subject to principles of coherence and sincere cooperation, conclude international agreements even if they are contrary to secondary law adopted by the European Parliament and the Council acting as co-legislators on a proposal of the Commission. To put it more crudely, if the GDPR is not the expression of the right to the protection of personal data as enshrined in Articles 7 and 8 CFR, there may be room for a doctrinal argument that the Council and the Commission could depart from the GDPR's standard when they negotiate (the Commission under a mandate from the Council) different rules with a third country.

A. Data Transfers and National Security

(i) Data Transfer to the USA: Schrems I *and the Privacy Shield*

The case of *Schrems I*[11] was in several respects a wake-up call, reminding us of the difficulties of protecting personal data once it has left the jurisdiction of the EU. Based on the DPD (because the GDPR had not yet been adopted) and on principled considerations drawn from Articles 7 and 8 CFR, the CJEU declared invalid the transfer regime between the EU and the USA.[12] It interpreted the adequate level of protection under the DPD as meaning an 'essentially equivalent' level of protection.[13]

The Commission found that data protection rules in the USA do not generally offer an adequate standard of protection but, with its 'adequacy' decision on the EU–US Safe Harbour regime (2000), endorsed the practice that companies self-certify that they meet a number of principles (safe harbour principles) and the US authorities check this within their competences.[14] The Commission had

[10] See also Case C-414/16 *Egenberger* ECLI:EU:C:2018:257 (Art. 21 and 47 CFR); Case C-569/16 *Bauer* ECLI:EU:C:2018:871 (Art 31(2) CFR).

[11] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.

[12] Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.

[13] Ibid, para 73–4.

[14] Decision 2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe

also repeatedly criticised the level of protection provided by the safe harbour regime,[15] and politically worked – albeit without great success – with the US authorities to improve it.[16] Relevant also for the public perception of data transfers to the USA were Edward Snowden's revelations in 2013 that under the PRISM programme the NSA is able to access personal data stored on US servers in an essentially unrestricted manner.

Max Schrems brought a complaint to the Irish DPA intended to stop the transfer of his personal data from Facebook Ireland to Facebook Inc in the USA. The Irish DPA declined to open an investigation because of the Commission's Safe Harbour Decision, despite the fact that the Decision confirmed the DPA's powers to stop data transfer in individual cases.[17] Schrems challenged the DPA's decision not to open an investigation before the Irish High Court, which referred a preliminary question to the CJEU. The Irish High Court specifically voiced doubts that US practices satisfied Articles 7 and 8 of the EU's CFR, as interpreted by the CJEU in *Digital Rights Ireland*.[18] In response, the CJEU emphasised the crucial role of national DPAs in the data protection framework within the EU,[19] and ruled that they had the obligation to investigate the level of protection in individual cases. If the national DPA finds fault with the data transfer, it must refer the case to a national court, which should ask a question to the CJEU as the only authority that can invalidate the Commission's adequacy decisions. The CJEU also invalidated the Commission's Safe Harbour Decision,[20] essentially because of the formal reason that the Safe Harbour regime was not based on legally binding obligations under either domestic US law or international law, but instead relies on a self-certification regime.

Moreover, the Court, recalling *Digital Rights Ireland*,[21] concluded that the Safe Harbour regime allowed for too far-reaching exceptions, including for national security matters. In essence, domestic law and international commitments of the third country would have to offer sufficient safeguards limiting the storage of personal data, access to that data by public authorities and further use of the data. Domestic law and international commitments would further have to offer remedies to individuals allowing them to access their data and, if need be, having it corrected or erased.

harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7 (Decision 2000/520/EC).

[15] Commission, 'Rebuilding Trust in EU–US Data Flows' (Communication) COM (2013) 846 final of 27 November 2013; Commission, 'The Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU' (Communication) COM (2013) 847 final of 27 November 2013.

[16] ibid.

[17] Art 3 of Decision 2000/520/EC.

[18] *Digital Rights Ireland* (n 7).

[19] See also Case C-288/12 *Commission v Hungary* [2014] ECLI:EU:C:2014:237.

[20] Art 25(6) DPD.

[21] *Digital Rights Ireland* (n 7).

After *Schrems I*, more than 4000 US companies, which had previously relied on the Safe Harbour regime, had to find new ways to continue making data transfers. Many switched to either Binding Corporate Rules or Standard Contractual Clauses (SCCs), both of which are more burdensome on the companies that use them and more limited in scope. SCCs are model clauses, approved by the Commission (SCC decision), that create contractual obligations between data controllers and data processors that govern the transfer of data. In 2016, the Safe Harbour regime was succeeded by the Privacy Shield. SCCs (and the Commission's SCC decision) remain relevant when businesses withdraw voluntarily from the Privacy Shield. The legal framework is construed to allow for derogation from an 'adequate' level of protection. It permits transfer of data to third countries which do not ensure an adequate level of protection on a more cumbersome case-by-case basis (SCC and SCC Decision).[22]

Besides the SCC, severe doubts about the adequacy of data protection under the Privacy Shield persist. Since its entry into force, several non-governmental organisations have tried and failed to challenge the Privacy Shield adequacy decision.[23] The Privacy Shield consists of 23 privacy principles,[24] together with official representations and commitments by various US authorities. It also relies on self-certification with the Department of Commerce. The Commission had confirmed the adequacy of the Privacy Shield within the framework established by the 1995 Data Protection Directive (Privacy Shield Decision 2016).[25]

Several institutional actors within the EU voiced concerns about the adequacy of the Privacy Shield. On 28 November 2017, the Article 29 Working Party, which has now been replaced by the European Data Protection Board, made recommendations to bring the Privacy Shield into compliance with the GDPR.[26] On 5 July 2018, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) adopted a non-binding resolution recommending that the Commission suspend the EU/US Privacy Shield unless the USA takes a number of specified steps to improve data protection.[27]

[22] Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council [2016] OJ L344/100.

[23] General Court, order of 22 November 2017, Case T-670/16 *Digital Rights Ireland v Commission*; action brought on 9 December 2016, Case T-738/16 *La Quadrature du Net and Others v Commission*.

[24] eg on data integrity and purpose limitation.

[25] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ L207/1, recital 13.

[26] Article 29 Data Protection Working Party, EU–US Privacy Shield – First Annual Joint Review, adopted 28 November 2017, WP 255/17 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.

[27] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU–US Privacy Shield (2018/2645(RSP)) www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018–0315&format=XML&language=EN.

The discussions demonstrate that a number of political actors remain doubtful about the level of protection offered under the Privacy Shield. The CJEU would certainly give additional fuel to these criticisms if it took the position in *Schrems III* that the data transfer to Facebook Inc was contrary to EU law, even if the case, narrowly construed, concerned data transfer under the SCC.

(ii) Data Transfers and National Security: Schrems III[28]

In his 2015 complaint to the Irish DPA, Max Schrems specifically alleged that his personal data transferred to the USA was 'made available to US Government authorities under various known and unknown legal provisions and spy programs such as the PRISM program'.[29] *Schrems III* hence specifically focuses on the consequences of the fact that US authorities access and process personal data originating in the EU for national security purposes. As Facebook Ireland was not relying on the Privacy Shield for transferring data of Mr Schrems to Facebook Inc in the USA, *Schrems III* directly only concerned transfers of data pursuant to SCC.

The Irish DPA had serious concerns with regard to the remedies offered for infringement, the restrictive standing requirements and the fact that the SCC were not binding on the US Government. It brought a case to the Irish High Court (*Schrems III*),[30] which found that the DPA raised well-founded concerns and again referred a question to the CJEU.[31] The Irish High Court inquired in particular whether the CFR applied to the transfer of personal data transferred from the EU to the USA for commercial purposes under SCCs and whether the possibility that this data is further processed for national security purposes infringes Articles 7, 8 and 47 CFR.

In the context of the investigations in *Schrems III*, five US experts,[32] selected by Max Schrems,[33] Facebook[34] and the Irish Data Protection Commissioner (DPC),[35] gave testimony, including more generally about the protection offered in the USA. Facebook's first expert, Swire, confirmed that the Foreign Intelligence Surveillance Court provides independent and effective oversight

[28] Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*.

[29] www.europe-v-facebook.org/comp_fb_ie.pdf.

[30] Case C-498/16 *Schrems II* [2018] ECLI:EU:C:2018:37 concerned jurisdictional matters and is irrelevant here.

[31] See *The Data Protection Commissioner v Facebook Ireland Ltd & anor* [2017] IEHC 545 http://courts.ie/Judgments.nsf/768d83be24938e1180256ef30048ca51/8131a5dde8baf9ff802581b70035c4ff?OpenDocument.

[32] https://iapp.org/resources/article/schrems-2–0-expert-testimony/.

[33] Ashley Gorski of the American Civil Liberties Union. https://iapp.org/media/pdf/resource_center/Schrems-testimony-Gorski.pdf.

[34] Professor Peter Swire of the Georgia Institute of Technology and Professor Stephen Vladeck of the University of Texas. Testimonies available at https://iapp.org/media/pdf/resource_center/Schrems-testimony-Swire.pdf and https://iapp.org/media/pdf/resource_center/Schrems-testimony-Vladeck.pdf.

[35] Testimonies not publicly available.

over US Government surveillance. Facebook's second expert, Vladeck, acknowledged shortcomings in the existing US legal regime with regard to redress of unlawful government data collection, but concluded that these shortcomings are not 'nearly as comprehensive – or that standing is as categorical an obstacle – as the DPC Draft Decision [and related materials] suggest'. What is certain is that the level of data protection in the USA is not at the same standard as in the EU and that EU's political institutions have no means, other than diplomatic and economic, to push for higher protection.

In *Schrems I*, the CJEU confirmed that the term 'adequate level of protection' in Article 25(6) of Directive 95/46/EC does not require a level of protection *identical* to the guarantees offered within the EU legal order. Instead, the third country must ensure a level of protection of fundamental rights that is 'essentially equivalent' to that guaranteed within the Union.[36] The means deployed may differ, but they must, in practice, prove effective. This allows for deviation, including not reaching the same level of protection in specific circumstances. This is thus the core question: does the USA offer an 'essentially equivalent' level of protection?

The Court has taken principled decisions not only in *Schrems I*, but in a much longer line of case law, even when this meant interrupting data transfer or the work of national security actors. It regularly forced political and economic actors to reconsider existing practices. Examples are the CJEU's rulings in *Digital Rights Ireland* and *Tele2*.

Digital Rights Ireland concerned the Data Retention Directive, which regulates the retention of metadata. Metadata is the information on a telecommunication, including location of the user, duration of the connection, subject-matter heading of emails and websites visited. It does not contain the personalised content of a communication. Prima facie, metadata may appear less problematic than personal data. However, in bulk, and with technically possible automated analysis tools, it can, in particular over time, amount to very sensitive information on a person.[37] Some interpreted *Digital Rights Ireland* as ruling that the general duty of retention is disproportionate.[38] Others argued that the Court accepted compensation for the general duty of retention by strict access requirements.[39]

The case of *Tele2* also concerned the retention of communications data and the necessary safeguards to protect it.[40] The issue was whether the Swedish and UK legislation imposing an obligation on public communications providers to retain traffic and location data was compatible with EU law. The Court used the standard of 'strictly necessary', and required that access to information be subject to a prior

[36] *Schrems I* (n 11) paras 73–74.

[37] I Cameron, 'Balancing Data Protection and Law Enforcement Needs: *Tele2 Sverige* and *Watson*' (2017) 54 *CML Rev* 1467, 1469 and references therein.

[38] ibid 1470ff.

[39] ibid.

[40] Joined Cases C-203/15 *Tele2 Sverige AB v Post- och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970; Cameron, 'Balancing Data Protection and Law Enforcement Needs' (n 37).

check by a court or independent authority, whose task it was to ensure that access was limited to requests that met this standard.[41]

Whether current practices meet an 'essentially equivalent' level of protection is precisely the issue in *Schrems III*. If the Court holds that current practices do not meet an 'essentially equivalent' level of protection, it will again be the task of the EU's political institutions and the US Government to find new ways of making data transfer possible and compliant with European data protection rights. First of all, this raises practical issues: is it, in practice, even possible to limit the access and processing rights of national security and law enforcement authorities of third states within the jurisdiction of the third state? Increasing mass surveillance and technological development will make this ever more difficult. Ultimately, compliance depends on the willingness of the third state. To ensure a certain entrenchment that makes non-compliance more difficult, the CJEU required national and international law commitments, rather than only administrative practice, in *Schrems I*.

Secondly, the underlying questions are: how far is it normatively justifiable to accept that private businesses transfer data to other countries in which the data subject is not able to enjoy the same level of protection? How far is it normatively justifiable to impose European data protection standards on businesses in – and, by extension, government authorities of – third countries? The answers to these questions are two sides of the same coin. The extraterritorial effects of European regulation and standards,[42] sometimes also called the Brussels effect,[43] is a hotly debated issue, not only in the area of data protection.

B. National Security Exemptions: A Blind Spot in the Checks and Balances of the EU's Data Protection System?

(i) National Security Exemptions and Substantive Standards of Protection

Schrems III specifically raised the question of whether the national security exemption in Article 4(2) TEU limited the application of EU data protection laws where national security is concerned and what the meaning of Article 3(2) Data Protection Directive, now Article 2(2) GDPR, is in this context.

Generally speaking, national security is a reserved national competence. This is expressed in Article 4(2) TEU, but also in recital 16 of the GDPR. However, the EU is competent to regulate commercial data transfers. Union and Member States then have the competence to derogate from EU law for reasons of national

[41] *Digital Rights Ireland* (n 7).

[42] C Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5 *International Data Privacy Law* 235.

[43] A Bradford, 'The Brussels Effect' (2012) 107 *Northwestern University Law Review* 1.

security (Article 3(2) DPD and Article 23 GDPR). These derogation clauses do not establish a standard of protection that needs to be complied with even in circumstances when national security concerns are argued. They only express the general commitment to the principle of proportionality. They are specifically addressed to the Union and the Member States.[44] Also, according to formal logic, these national security exemptions under EU law – that is, clauses that allow derogation from EU law – can only apply to the exercise of public power by authorities of those bound by EU law – that is, Member States – and hence arguably only for the purpose of protecting the national security of the Member States (and possibly the EU). The derogation clauses do not apply directly to third states or their national security authorities.

Prima facie, this leaves third countries in a position where they cannot directly rely on any national security exemption under EU law. What rules should then apply to access and processing of personal data of EU citizens by national security and law enforcement authorities of third states? This is what Article 45 GDPR addresses when regulating data transfers to third countries that offer adequate protection. Adequate protection means in particular that access and processing of personal data for national security and law enforcement purposes is regulated in that third country in a way that offers essentially equivalent protection.

Even when Member States rely on national security concerns within the scope of the GDPR and derogate from the usual data protection rules, they remain bound by EU law. Within the Union's system of fundamental rights protection, the two core questions are: is the CFR applicable? Is the ECHR applicable?

The application of the CFR is limited to actions of the Member States when they implement EU law (Article 51 CFR). This has been interpreted by the CJEU as meaning 'within the scope of EU law'[45] and continues to be interpreted roughly along the same lines as in the CJEU's pre-Lisbon Treaty case law,[46] arguably clarifying that it is sufficient that EU law objectives are affected.[47] When Member States derogate from EU law – that is, within the scope of application of the GDPR – their actions must comply with the CFR. In principle, however, when Member States exercise reserved competences and pursue national security objectives (eg data processing that does not fall within the scope of the GDPR), their actions do not fall within the scope of EU law.[48] However, even then they do not act in a law-free space.

First of all, the ECHR is in principle applicable to all actions of the Member States, irrespective of the scope of EU law and irrespective of the competence division between the EU and its Member States. Article 8 ECHR protects personal data and restricts storage and use of personal data. Article 15 ECHR allows,

[44] Art 23 GDPR.

[45] See C-617/10 *Fransson* ECLI:EU:C:2013:280; C-206/13 *Siragusa* ECLI:EU:C:2014:126.

[46] Case 5/88 *Wachauf* ECLI:EU:C:1989:321; Case C-260/89 *ERT* ECLI:EU:C:1991:254.

[47] See *Fransson* (n 45); *Siragusa* (n 45).

[48] Case C-446/12 *Willems* ECLI:EU:C:2015:238 illustrates that where a Member State uses data collected under an EU regulation for purposes outside that regulation, it acts outside of the scope of EU law.

in exceptional cases, for a declaration of a state of emergency, which leads to a general restriction of Convention rights; yet, the state of emergency exception is not applicable to the current discussion. The Irish High Court inquired whether the ECHR was directly applicable through EU law.[49] Secondly, the CJEU clarified that Member States, also when exercising their reserved competences, are bound by a general duty to respect the founding provisions of EU law, including general principles.[50]

The issues of mass surveillance and data transfers to third countries have been brought not only before the CJEU, but also before the European Court of Human Rights (ECtHR). The ECtHR confirmed in the cases of *Zakharov* and *Szabo* how seriously it takes data protection.[51] In early 2019, two relevant cases were referred to the Grand Chamber of the ECtHR. The first concerns complaints by journalists, individuals and rights organisations about three different surveillance regimes: (i) the bulk interception of communications; (ii) intelligence sharing with foreign governments; and (iii) the obtaining of communications data from communications service providers.[52] The second concerns a complaint brought by a public interest law firm alleging that legislation permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes breached its privacy rights.[53] So far, no specific principles have been developed that could give useful guidance on the point of how far personal data could and should be protected beyond the jurisdiction of the contracting parties of the ECHR. Yet, the pending cases give the ECtHR further occasion to develop the right to data protection in Europe.

EU Member States hence remain bound by the right to the protection of personal data under the ECHR, including when EU law does not apply. Even when acting with the objective of protecting national security, they must continue to adhere to the ECHR. Within the EU, this general commitment to a shared interpretation of human rights protection is also the very basis of mutual trust between Member States, on which all cooperation, including data exchange, depends.

(ii) Checks and Balances within the EU

The CJEU's data protection case law also has repercussions for the balance of powers within the EU. *Schrems I* is an example of decentralisation of power to the

[49] See formulation of question 1: http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6451273.

[50] See Case C-192/05 *Tas-Hagen and Tas* ECLI:EU:C:2006:676; Case C-135/08 *Rottmann* ECLI:EU:C:2010:104; Case C-438/05 *Viking* ECLI:EU:C:2007:772. For an ongoing discussion of the relevance of general principles beyond the scope of the Charter, see C Amalfitano, *General Principles of EU Law and the Protection of Fundamental Rights* (Cheltenham, Edward Elgar Publishing, 2018).

[51] *Zakharov v Russia* App no 47143/06 (2016) 63 EHRR 17 (ECtHR, 4 December 2015); *Szabo v Hungary* App no 37138/14 (2016) 63 EHRR 3 (ECtHR, 12 January 2016).

[52] *Big Brother Watch and Others v the United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).

[53] *Centrum för rättvisa v Sweden* App no 35252/08 (ECtHR, 19 June 2018).

Member States. Article 25(6) DPD confers a power on the Commission to make a finding that a particular third country ensures an adequate level of protection so that, in principle, personal data may be transferred from any EU Member State to a non-EU state. It remains the task of the national DPA to ensure that the level of protection in the individual case is adequate pursuant to the criteria set out in Article 25(2) DPD.[54]

The Court confirmed the important role of national DPAs under this framework and emphasised that it needs to conduct autonomous inquiries into the level of data protection in each individual case, even if the Commission has overall found the transfer regime adequate.

Tele2, by contrast, is a case in which more decentralisation would have been possible and desirable. The AG in *Tele2* suggested more decentralisation. The Court rejected the AG's Opinion; however, the Court's decision in this regard has been criticised.[55]

Decentralisation and shared responsibilities at different levels of government introduce a mechanism of checks and balances, which seems capable of contributing significantly to the overall level of protection. At the same time, the way the control mechanism is constructed in *Schrems I*, ultimately requiring a reference to the CJEU, makes it highly likely that data protection cases end up before the Court of Justice. This allows the Court to develop and enforce a uniform level of protection. It is also inevitably a form of centralisation. Overall, the mechanism of checks and balances inherent in the EU's legal framework for data protection involves a number of different authorities with the mandate to ensure and enforce a high level of protection. It seems prone to strengthen the level of protection over time rather than to lower it.

C. Concluding Remarks

Both 2018 and 2019 have been characterised by increasing geo-economic tensions, such as sanctions, tariffs, free trade agreements and investment protection. Data flows across the globe continue to grow exponentially. Commercial data is of ever greater economic relevance, and any limitations imposed by the CJEU or any other EU institution are likely to be received as actions that form part of this growing tension. Data is not only used for law enforcement purposes, but is also highly relevant, for example, for the good functioning of democracies, including national elections in EU Member States and elections to the European Parliament. This is the context in which the debate on protection of personal data after commercial data transfers should be placed.

The CJEU has time and again upheld EU data protection standards in different situations – when data is transferred to third countries (*Schrems I*), when data

[54] Art 25(1) DPD.
[55] Cameron (n 37).

is accessed and processed by telecommunications providers (*Tele2*) and when data is retained, including for future law enforcement purposes (*Digital Rights Ireland*). It is certain that the EU data protection standards do not apply when data is transferred to third countries and that the EU has only limited means to enforce the agreements made with the third country. Requiring the same standard would be practically impossible. It would also raise normative questions if US authorities would have to act pursuant to EU standards, adopted by political representatives of the EU and national citizens. The question remains what is an essentially equivalent level of protection and how can it be ensured in practice? This is what is necessary in order to justify allowing commercial data transfers on a large scale.

III. Impunities Surrounding the Deployment of Liaison Officers

A. Legal Basis and Tasks of Liaison Officers

Cooperation and coordination between police, judicial authorities and other competent authorities within the AFSJ is one of the core objectives laid down in the TFEU to ensure security in the EU.[56] The many challenges stipulated in the Treaties reflect the EU's growing international perspective. Over the past two decades, cooperation between the EU and third countries has increased sharply.[57] Correspondingly, a significant amount of EU secondary law and EU (policy) documents on security and migration[58] stresses the importance of cooperation between competent authorities between the EU and external actors. To establish

[56] Art 67(3) TFEU on criminal matters in the area of freedom, security and justice.

[57] J Monar, 'The EU's Growing External Role in the AFSJ Domain: Factors, Framework and Forms of Action' (2014) 27 *Cambridge Review of International Affairs* 147, 149; RA Wessel, L Marin and C Matera, 'The External Dimension of the EU's Area of Freedom, Security and Justice' in C Eckes and T Konstadinides (eds), *Crime Within the Area of Freedom, Security and Justice: A European Public Order* (Cambridge, Cambridge University Press, 2011), 277.

[58] Recitals 1, 3 and 4 of Council Regulation (EC) 377/2004 of 19 February 2004 on the creation of an Immigration Liaison Officers network [2004] OJ L64/1 (ILO Regulation); Art 54 and recital 20 of Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard [2016] OJ L251/1 (Frontex Regulation); concluded bilateral agreements between Frontex and third countries: Canada, Turkey and the USA; C Jones, 'Briefing: Frontex: Cooperation with Non-EU States' (*Statewatch*, March 2017) www.statewatch.org/analyses/no-309-frontex-third-countries-agreements.pdf, 12; Art 8(3) of Regulation (EU) 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation [2016] OJ L135/53 (Europol Regulation).

Council of the European Union report, 'Outcome of the EU – US Justice and Home Affairs Senior Officials Meeting, Valetta 1–2 March 2017'; Commission, 'Establishing a New Partnership Framework with Third Countries under the European Agenda on Migration' (Communication) COM (2016) 385 final; Commission, 'Proposal for a Regulation of the EP and the Council on the Creation of a European Network of Immigration Liaison Officers' COM (2018) 303.

and maintain links between EU and third-country authorities, one of the instruments used is the deployment of liaison officers from third countries within the EU and vice versa.[59] The objective and tasks for liaison officer secondment focuses on 'coordination and cooperation between police and judicial authorities'.[60] This is in line with the objectives stipulated in the general provisions on the AFSJ set out in the TFEU.

The deployment of liaison officers is based on a variety of legal instruments: EU Regulations,[61] bilateral cooperation agreements[62] and Memoranda of Understanding[63] concluded between an EU authority and a third-country authority, often in the areas of security or migration. The instruments are, however, ambiguous about which is the competent jurisdiction that subjects liaison officers to administrative or judicial review, as well as the applicable legal regime. As it is unclear which legal regime implicitly or explicitly applies to the liaison officer, it is also unclear what data protection standards apply to them.

The same legal instruments list generally defined tasks of liaison officers, but fail to qualify their actual reach or legal effect, which is relevant in determining what rules and consequent control mechanisms may apply to these liaison officers. A wide array of responsibilities for liaison officers are visible in annual reports of EU AFSJ agencies[64] and job vacancies for liaison officers.[65] The responsibilities vary from far-reaching (ie use of EU and Member State databases for police and migration purposes;[66] assistance and facilitation of the swift exchange of information;[67]

[59] HCH Hofmann and AH Türk, *EU Administrative Governance* (Cheltenham, Edward Elgar Publishing, 2006) 343.

[60] Art 27(3) of the Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime [2002] OJ L63/1 (hereafter Eurojust Dec); Art 8(1) Europol Regulation; ArtArt. 12(3) and 54 Frontex Regulation.

[61] Europol Regulation (ibid); ILO Regulation (n 56).

[62] Two types of cooperation agreement exist in the legal interaction between EU AFSJ agencies and non-EU states or other entities outside the EU: strategic and operational agreements. Both types of agreement are aimed at enhancing cooperation between the EU agency and the non-EU state concerned. There is, however, one major difference: strategic agreements do not allow for the exchange of personal data, whereas the operational agreements do. See, eg the Annexes to the Europol cooperation agreements (n 72 and n 96).

[63] Interpol–Europol Memorandum of Understanding; Memorandum of Understanding between Eurojust–United Nations Office on Drugs and Crime (UNODC).

[64] Europol, *Europol Review 2016–2017* (2018) 64; Frontex, *A Year in Review: First 12 Months of the European Border and Coast Guard Agency* (2017) 3–5.

[65] See, eg the job vacancy for British immigration liaison officers posted 17 May 2016 by the British High Commission Office – Foreign and Commonwealth Office under https://fco.tal.net/vx/mobile-0/appcentre-ext/brand-2/candidate/so/pm/4/pl/1/opp/368-Immigration-Liaison-Officer/en-GB (job advertisement no longer available).

[66] Art 8(3), (4) Europol Regulation; exchange of information via liaison officers, via long established channels between EU Member States and third countries: 'Europol–USA Agreement: Was It Really Needed?' (*Statewatch*, 2006) www.statewatch.org/news/2006/jul/01europol-usa.htm.

[67] Art 8(3) Europol Regulation; Art 2(1) Council Regulation 377/2004; Council of the European Union outcome report, 'Meeting with Eurojust Contact Points and Liaison Magistrates appointed by Member States: Complementarity, Synergies and Cooperation, 16–17 October 2014' (20 February 2015) 4 www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategicmeetings/Outcome%

providing support for the decision quality of visa decisions[68]) to less far-reaching (ie network building;[69] advisory roles[70]).

B. Liaison Officers: A Short Introduction

A specific, highly relevant, but relatively unexplored tool in crime prevention cooperation is the secondment of liaison officers in the EU's area of freedom, security and justice (AFSJ). The deployment of liaison officers raises data protection concerns that could be characterised as the flipside of those discussed in the first section on commercial data transfers. It does not primarily concern what happens to data once it has left the jurisdiction of the EU and its Member States, but it does concern whether and how EU data protection rules apply to administrative officers from third countries, when they work within the EU administration and within the EU's jurisdiction.

Liaison officers are administrative agents who connect two or more administrative authorities of different jurisdictions. It is their objective to support their home administration in the enforcement of its laws. This support manifests itself in cooperation and coordination actions mainly situated in the area of security, justice and migration.The home administration is an executive body responsible for administration or enforcement in a particular policy area that deploys a liaison officer to a receiving (host) administration.[71] Once at the host administration, liaison officers carry out multiple executive tasks entrusted to them. One of those tasks discussed more extensively in this section is the easing of a swift exchange of (non)-personal information between the home and host administration. This practice of data transfers via liaison officers highlights conflicting legal issues. When liaison officers are deployed from third countries to administrative authorities within the EU, it becomes unclear under which jurisdiction they fall and what data protection rules apply. These 'non-EU state' liaison officers are in many cases regarded as a 'formal representative' of the sending administration.[72] They fall outside the EU's data protection framework described above. Put differently: liaison officers

20report%20of%20the%20meeting%20with%20Eurojust%20Contact%20Points%20and%20Liaison%20Magistrates%20(16–17%20October%202014)/Outcome-report_EJ-contact-points-liaison-and-magistrates-meeting_2015–02–20_EN.pdf.

[68] British Immigration liaison officer job vacancy (n 65).

[69] E Aydinli and H Yön, 'Transgovernmentalism Meets Security: Police Liaison Officers, Terrorism, and Statist Transnationalism' (2011) 24 *Governance: An International Journal of Policy, Administration and Institutions* 66, 67.

[70] Council outcome report, 'Meeting with Eurojust Contact Points and Liaison Magistrates' (n 67).

[71] Liaison officers can also be seconded in other policy areas to ease cooperation between administrations, such as in the areas of migration and justice.

[72] Art 2(1), Annex 4 of the Agreement on Operational and Strategic Co-operation between the Republic of Colombia and the European Police Office; Art 2, Annex III of the Agreement on Operational and Strategic Co-operation between the Government of HSH the Sovereign Prince of Monaco and Europol; Art 2, Annex III of the Agreement between the Republic of Iceland and Europol.

seconded from third countries are exempted from EU data protection standards, including when they act within the EU.

C. Liaison Officers as Intermediate Agent in the Area of Freedom, Security and Justice: The Example of Europol

Cooperation between the EU AFSJ agencies is necessary to enable large-scale collaboration in the fight against crime. AFSJ agencies are executive, specialised bodies constituted under Title V of the TFEU and responsible for the enforcement EU laws in that specific field.[73] The scope of cooperation in the field of security has increasingly developed beyond the EU's external borders and pushes the EU to cooperate with third-country security agencies. This changing landscape towards more cooperation with third-country authorities is already subject to an extensive scholarly debate in different areas such as human rights,[74] conflict of jurisdictions[75] and the application of EU data protection standards.[76] Liaison officers are, however, sidelined in that debate. A thorough study of US liaison officers seconded to Europol is therefore specifically interesting when linked to impunity from data protection standards.[77] This is a space in EU law where the European data protection standards do not apply, including within the EU administration when and because external actors are involved.

Europol is a particularly pertinent example highlighting these spaces where external agents – that is, US liaison officers – retrieve data from the EU administration and transfer it to their home administration. Europol is designed to operate in partnership with law enforcement agencies, government departments *and* the private sector.[78] This further widens the potential access of third-country liaison officers to EU data when they are deployed to Europol. In the close cooperation between public and private parties for law enforcement purposes, liaison officers act as intermediaries with a broad formal and informal network to get access to data regarded as necessary. To give some insight into the numbers of non-EU state liaison officers based in the EU: 243 liaison officers are placed at Europol, 51 of

[73] Agencies established on the basis of the TFEU articles on the area of freedom, security and justice: Europol, Eurojust, Frontex and, in the future, the European Public Prosecutors Office (EPPO).

[74] M Fink, 'Frontex Working Arrangements: Legitimacy and Human Rights Concerns Regarding Technical Relationships' (2012) 28 *Merkourios-Utrecht Journal of International and European Law* 20; JJ Rijpma, 'External Migration and Asylum Management: Accountability for Executive Action Outside EU Territory' (2017) 2 *European Papers* 571.

[75] M Böse, 'EU Substantive Criminal Law and Jurisdiction Clauses: Claiming Jurisdiction to Fight Impunity?', ch 5 in this book.

[76] M Eliantonio, 'Information Exchange in European Administrative law: A Threat to Effective Judicial Protection?' (2016) 23 *Maastricht Journal of European and Comparative Law* 531.

[77] The Europol website mentions, among others, FBI, Secret Service, NYPD, US customs authorities: www.europol.europa.eu/partners-agreements.

[78] ibid.

whom are deployed from third countries.[79] This is not a negligible proportion of the total amount of 1294 Europol employees. When non-EU state liaison officers access databases set up and maintained in the EU's geographical jurisdiction, to what extent is that data protected under the EU data protection rules, as specified in EU secondary law and the case law of the Court of Justice? The following section shows the differences in the selection and deployment procedures of liaison officers seconded by an EU Member State and those seconded by a third country to Europol.

(i) Selection Procedure for EU Member State Liaison Officers

Liaison officers function as a 'hub for information exchange between the law enforcement authorities for the EU Member States'.[80] Every EU Member State is obliged to select and deploy at least one liaison officer to Europol.[81] Europol's Founding Regulation provides some rules on the procedure for secondment of Member State liaison officers to Europol.[82] First, each EU Member State establishes or designates a national unit to function as the liaison body between Europol and the competent authorities of that Member State. The national unit is led by an official appointed by the Member State.[83] A Member State national unit must be competent under national law to fulfil the tasks assigned in the Regulation, which mainly boil down to a very broad 'coordinating role' and 'cooperation between Member States'.[84] This means in particular facilitating access to national law enforcement databases and other relevant data necessary for cooperation with Europol.[85] The organisation and staff of a particular national unit is subject to national law.[86] As an exemption to this rule, Member States may still allow direct contacts between their competent authorities and Europol – and may directly exchange information – without involvement of the national unit.[87]

The second step of liaison officer deployment is their designation by the respective national unit to Europol.[88] It is not clear from the Regulation, however, if the national unit designates a liaison officer from the national unit itself or from one of the competent authorities of the Member State. What is clear, though, is that the national unit instructs liaison officers.[89] In any case, Member States' liaison officers are subject to the national law of the designating Member State and remain subject

[79] www.europol.europa.eu/about-europol/statistics-data.
[80] Art 7(3) and recital 3 Europol Regulation.
[81] Art 8(1) Europol Regulation.
[82] Art. 7 and 8 Europol Regulation.
[83] Art 7(2) Europol Regulation.
[84] Recital 14 Europol Regulation.
[85] Art 8(3) Europol Regulation.
[86] Art 7(4) Europol Regulation.
[87] Art 7(5) Europol Regulation.
[88] Art 8(1) Europol Regulation.
[89] Art 8(2) Europol Regulation.

to the EU data protection framework.[90] That premise is relevant for non-EU state liaison officers seconded to Europol – they remain subject to their national law, and hence to their own national data protection standards.

(ii) US Liaison Officers Seconded to Europol

The Europol Founding Regulation provides rules for the conclusion of cooperation agreements between Europol and third countries.[91] These types of arrangements allow the exchange of non-personal and personal data to 'the extent necessary to fulfil the tasks' of Europol.[92] The selection and secondment of non-EU state liaison officers to Europol is also regulated in these cooperation agreements. Often, they refer to an annex or liaison agreement that specifies the tasks, status and obligations of liaison officers. The USA concluded such an operational agreement with Europol in 2001, in which the secondment of liaison officers is laid down.[93] The cooperation agreement (labelled the '2001 Agreement') states vaguely that the liaison officers' functions, tasks and status will be subject to consultations with a view to concluding a liaison agreement. The questions arise what specific parties are involved in these 'consultations', as the liaison agreement is still closed from public view,[94] and how data protection is arranged in case of (personal) information exchange. The exchange of personal data and data protection is arranged in a supplemental agreement to the 2001 Agreement, but contains a large number of ambiguities related to data protection. The next section outlines these ambiguities and other spaces in law in which the US liaison officers transfer data to the USA.

D. Do European Data Protection Standards Apply to US Liaison Officers at Europol?

US liaison officers deployed at Europol are not subject to the same level of European data protection rules. In essence, the USA–Europol cooperation agreement allows the exchange of personal data,[95] despite the fact that the personal data is not protected by EU data protection rules during and after the transfer. The following subsection sets out the legal structure under which US liaison officers (and other non-EU state liaison officers) operate when seconded to Europol.

[90] Art 8(3) and (4) Europol Regulation.
[91] Art 25 Europol Regulation.
[92] Recital 32 Europol Regulation.
[93] Art 8 of the Agreement between the United States of America and the European Police Office.
[94] This is different from other cooperation agreements with third countries, eg the Agreement between the Kingdom of Norway and the European Police Office.
[95] www.europol.europa.eu/newsroom/news/today-brazil-and-europol-signed-agreement-to-expand-cooperation-to-combat-cross-border-criminal-activities.

(i) Gaps in European Law Regarding Information Exchange

US liaison officers seconded to Europol are not subject to the laws and regulations of the EU that lay down data protection rules within the EU. Like many other non-EU state liaison officers deployed at Europol, US liaison officers are a formal representative of the USA with respect to Europol.[96] Not being members of the Europol staff themselves and subject to their own national laws, US liaison officers do not, for example, fall under the general Regulation 2018/1725 applicable to the Union institutions, bodies, offices and agencies who process personal data.[97] The scope of the Data Protection Regulation for EU institutions reveals that it does not apply to the processing of operational personal data by Europol.[98] In addition, the Europol Regulation explicitly allows data transfers between Europol and third countries on the basis of cooperation agreements concluded between the two administrations.[99]

Furthermore, the above-introduced GDPR does not apply since competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences are exempted.[100] This means that an adequacy decision – in the US case, the Privacy Shield framework – does not apply to the law and practices of US liaison officers either. In the above-discussed context, the Privacy Shield protects EU personal data that is transferred to the USA for commercial purposes. It is not relevant for data transferred for law enforcement purposes. Directive 2018/680 on data processing by competent authorities for the purposes of law enforcement does not apply either, as the addressees are the EU Member States and (understandably) not third countries. The Umbrella Agreement does apply to personal data transferred between US liaison officers and Europol, but does not provide the same level of data protection. Hence, a legal vacuum in data protection standards is revealed in the case of US liaison officers deployed at Europol.

(ii) Data Protection Standards in the Supplemental Agreements?

As intermediaries between two agencies, liaison officers seconded from US security agencies to Europol carry out tasks outside the scope of application of EU rules on data protection. Data protection rules that apply to the law enforcement cooperation arrangement between the USA and Europol, on the basis of

[96] This is acknowledged in other cooperation agreements: Art 2(1), Annex 4 of the Colombia–Europol cooperation agreement; Annex to the Moldova–Europol cooperation agreement; Art 2(1), Annex 4 of the cooperation agreement between the Former Yugoslav Republic of Macedonia and Europol.

[97] Regulation (EU) 2018/1725 of 23 October 2018 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data [2018] OJ L295/39.

[98] Ibid Art 2(3). The exemption of Europol is of a temporary nature.

[99] Art 25(3) Europol Regulation.

[100] Art 2(2)d GDPR.

which liaison officers are seconded, are laid down in the supplemental agreement between Europol and the USA on the exchange of personal data.[101] The agreement has a broad scope under which the parties may exchange information, including personal data, in accordance with the provisions of the agreement.[102] However, the agreement lacks basic data protection standards, such as control or supervisory mechanisms of the actors responsible for data transfers between the two administrative authorities. In vague terms, the agreement states that information supplied by Europol 'shall be available to competent US federal authorities' and available for use by competent US state or local authorities, provided that they agree to observe the provisions of the agreement.[103] How this practice of data use is supervised or controlled remains, however, ambiguous. US liaison officers seconded to Europol are not covered by EU data protection rules. They are subject to their national data protection laws, though these are, as argued earlier in this chapter, not the same as the European data protection standards.

IV. Conclusions: Impunities from Data Protection?

This chapter has identified what rules apply to data cooperation with the USA in two illustrative cases of commercial data transfers and liaison officers. The two cases illustrate two sides of the same coin: data protection when data leaves the jurisdictions of the EU and its Member States to the USA, and when external officers – that is, US liaison officers – are deployed to the EU administration. The chapter demonstrates that in both cases the level of data protection is not the same as within the jurisdictions of the EU and its Member States. It also highlights the difficulties of ensuring a sufficient level of protection or even establishing what rules precisely apply and who applies them.

One conclusion is that it lies in the nature of the involvement of third countries that gaps and impunities cannot be fully ruled out. International cooperation both in the context of commercial data transfers and in the context of law enforcement cooperation has become more and more widespread, relevant and even unavoidable in the past decades. The remaining question is: how can a sufficient level of data protection be ensured? How can the EU institutions ensure that certain rules apply?

In the context of commercial data transfers, the problem of ensuring sufficient protection of personal data of EU citizens continues to persist even after the Court of Justice has interfered and after several political attempts were made in order to achieve better and more formal guarantees of data protection from the

[101] Supplemental Agreement between the Europol Police Office and the United States of America on the Exchange of Personal Data and Related Information.
[102] Art 3(1) Supplemental Agreement.
[103] Art 7(1) a and b Supplemental Agreement.

US Government. US companies have shown willingness to comply with EU rules, even if under US law they are not legally obliged to do so.[104] However, in particular the rules on access of national security agencies to data of EU citizens collected by commercial actors and judicial protection from infringements of data protection rights in the USA remain issues that are approached very differently in the EU and in the USA. Both issues further are not in the hands of commercial actors. In fact, commercial actors in the USA are often not in the position to deny access by national security agencies.

EU secondary law and the case law of the CJEU take a decentralised approach, in which both the European Commission and national DPAs both play a role in assessing the level of protection. The Commission makes a general assessment of the situation in the third country and 28 national DPAs assess the individual case. Together, this division of tasks seems to pave the way for a race to the top rather than a race to the bottom.

In the context of US liaison officers seconded to the EU, the greatest problem is the level of unclarity of the rules applying to data transfers. The cooperation agreement concluded between Europol and the USA contains a vast, multi-interpretable list of areas of crimes that allow the exchange of information. This has the consequence that data protection rights are not safeguarded with the same legal certainty and at a level comparable to the level guaranteed within the EU. A question for further examination that is equally highly relevant in this context is what control or accountability rules actually apply to non-EU state liaison officers.

[104] F Marotta-Wurgler, 'Understanding Privacy Policies: Content, Self-Regulation, and Markets' (2016) New York University Law and Economics Working Papers 4–2016 https://lsr.nellco.org/cgi/viewcontent.cgi?article=1439&context=nyu_lewp.