



UvA-DARE (Digital Academic Repository)

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](https://doi.org/10.2139/ssrn.3493611)
[10.5040/9781509926909.ch-017](https://doi.org/10.5040/9781509926909.ch-017)

Publication date

2020

Document Version

Submitted manuscript

Published in

The Fight Against Impunity in EU Law

[Link to publication](#)

Citation for published version (APA):

Eckes, C., & Barnhoorn, D. (2020). Commercial Data Transfers and Liaison Officers: What Data Protection Rules Apply in the Fight against Impunity When Third Countries Are Involved? In L. Marin, & S. Montaldo (Eds.), *The Fight Against Impunity in EU Law* (pp. 317-337). (Hart Studies in European Criminal Law). Hart. <https://doi.org/10.2139/ssrn.3493611>, <https://doi.org/10.5040/9781509926909.ch-017>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)



UNIVERSITY OF AMSTERDAM



AMSTERDAM
CENTRE FOR
EUROPEAN
LAW AND
GOVERNANCE

COMMERCIAL DATA TRANSFERS AND LIAISON OFFICERS: WHAT DATA PROTECTION RULES APPLY IN THE FIGHT AGAINST IMPUNITY WHEN THIRD COUNTRIES ARE INVOLVED?

Christina Eckes

Dominique Barnhoorn

Amsterdam Law School Legal Studies Research Paper No. 2019-42

Amsterdam Centre for European Law and Governance Research Paper No. 2019-04

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, University of Amsterdam

Summary:

This contribution addresses the question of whether and under what circumstances data protection should prevail over the fight against impunity. It focusses on data cooperation between the European Union and the United States of America (US) 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 US to EU agencies within the Area of Freedom Security and Justice (AFSJ). 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 21st century.

1. Introduction

Data protection is one of the great challenges of the 21st century. More and more data is stored, transferred, sold, and analysed. It is used to enforce the law, 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 to work in its agencies and have access to data, 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.

This contribution addresses the question of whether and under what circumstances data protection should prevail over the fight against impunity. It focusses on data cooperation between the European Union and the United States of America (US) 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 US to EU agencies within the Area of Freedom Security and Justice (AFSJ). 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 21st century.

The paper is structured as follows. The **first part** briefly sketches the EU's legal framework for data protection. The **second part** 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

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

(CJEU)'s recent case law on data protection, including the cases of *Schrems I (2015)* and *Schrems III (pending)* 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. Part two 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. The **third part** of the paper focusses on the specific example of data transfers via liaison officers in the AFSJ. Liaison officers are introduced as intermediate actors between two administrations, in the relevant case Europol and the US administration. It examines whether and how EU data protection standards could apply to liaison officers deployed from the US to Europol. The **conclusion** argues that protection of data that leaves the jurisdiction of the EU cannot be guaranteed at the same level as 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 EU 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.

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) 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 2016 Directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes.²

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 a general 'adequacy decisions' that address the general level of protection within the third country.⁵ The DPAs examine specific requests from individuals. 'Adequacy' implies that the standard does not

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 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) of the DPD; Art 45(1) of the GDPR.

⁵ Art 25(6) of the DPD; Art 45(1) of the GDPR, see also recitals 103-7, emphasizing the Commission's role and the EU's commitment to fundamental rights.

have to be the same but that in fact data transfer is legal when a *different*, that is also lower, standard applies after the data has left the jurisdiction of the EU.

In 2016, the EU concluded an umbrella agreement with the US on data transfers to the US for law enforcement purposes. The EU placed a number of demands on the US 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 US also adopted the US Freedom Act 2015. However, it is fairly uncontroversial that domestic legal rules in the US 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 generalized basis, which was specifically found illegal under EU law (*Digital Rights Ireland (2014)*),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 US 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 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 can as such 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 US could disregard the protection provided under the GDPR.

If this was 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.

⁶ Judicial Redress Act of 2015.

⁷ Joined Cases C-293 & 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] EU:C:2014:238.

⁸ Art 8 CFR.

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

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

1.2.Data Transfers and National Security

1.2.1. Data Transfer to the US: *Schrems I and the Privacy Shield*

The case of *Schrems I (2015)*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 Article 7 and 8 CFR, the CJEU declared invalid the transfer regime between the EU and the US.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 US do not generally offer an adequate standard of protection but endorsed with its 'adequacy' decision on the EU-US Safe Harbour regime (2000) 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 also had repeatedly criticized the level of protection provided by the safe harbour regime,¹⁵ and politically worked – without great success – with the US authorities to improve it.¹⁶ Relevant also for the public perception of data transfers to the US 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 US. The Irish DPA declined to open an investigation because of the Commission’s Safe Harbour Decision, despite the fact that the Commission’s Safe Harbour 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 CFR, as interpreted by the CJEU in *Digital Rights Ireland*.¹⁸ In response, the CJEU emphasized 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

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

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

¹³

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

¹⁵ Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final of 27 November 2013; Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final of 27 November 2013.

¹⁶ *Ibid.*

¹⁷ Art 3 of Decision 2000/520/EC.

¹⁸ Joined Cases C-293 & 594/12, *Digital Rights Ireland* (n 6).

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

²⁰ Art 25(6) DPD.

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.

After *Schrems I*, more than 4,000 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. SCC (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 NGOs have tried and failed to challenge the Privacy Shield adequacy decision.²³ The Privacy Shield consists of 23 privacy principles,²⁴ together with the 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 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 is now replaced by the European Data Protection Board, made recommendations to bring the Privacy Shield in compliance with the GDPR.²⁶ On 5 July 2018, the European Parliament's Committee on Civil

²¹ Joined Cases C-293 & 594/12, *Digital Rights Ireland* (n 7).

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 E.g. 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.

Liberties, Justice and Home Affairs (LIBE Committee) adopted a non-binding resolution recommending that the Commission suspend the EU/US Privacy Shield unless the US takes a number of specified steps to improve data protection.²⁷

The discussions demonstrate that a number of political actors remain doubtful about the level of protection offered under the Privacy Shield. The Court 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.

1.2.2. 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 US 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 US, *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 referred again 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 US 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 US. Facebook’s first expert, Swire, confirmed that FISC provides independent and effective oversight 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

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

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

²⁹ http://www.europe-v-facebook.org/comp_fb_ie.pdf.

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

³¹ See: *The Data Protection Commissioner v Facebook Ireland Ltd & anor* [2017] IEHC 545 <http://courts.ie/Judgments.nsf/768d83be24938e1180256cf30048ca51/8131a5dde8baf9ff802581b70035c4ff?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.

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 US is not at the same standard as in the EU and that EU’s political institutions have no other than diplomatic and economic means 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 prove, in practice, effective. This allows for deviation, including not reaching the same level of protection in specific circumstances. This is hence the core question: does the US offer an ‘essentially equivalent’ level of protection.

Not only in *Schrems I*, but in a much longer line of case law the Court has taken principled decisions, including 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* (2014) and *Tele2* (2016).

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, websites visited. It does not contain the personalized content of a communication. *Prima facie*, metadata may appear less problematic than personal data. However, in bulk and with technical 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* equally 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 handled the standard of ‘strictly necessary’ and required that access to information be subject to a prior check by a court or independent authority whose task it is to ensure that access is limited to requests that meet 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 be – again – the task of the EU’s political institutions and the US Government to find new ways of making data transfer possible and compliant with

³⁶ *Schrems I*, paras 73-4.

³⁷ Iain Cameron, ‘Balancing data protection and law enforcement needs: *Tele2 Sverige* and *Watson*’ (2017) 54(5) CMLRev 1467, 1469 with further references.

³⁸ *Ibid*, p. 1470 ff.

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* [2016] EU:C:2016:970. Iain Cameron, ‘Balancing data protection and law enforcement needs’, *ibid*.

⁴¹ Joined Cases C-293 & 594/12 *Digital Rights Ireland* (n 6).

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 in *Schrems I* national and international law commitments, rather than only administrative practice.

Second, the underlying questions are however: 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 Brussels effect,⁴³ is a hotly debated issue, not only in the area of data protection.

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

2.1. 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.

National security is generally speaking 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 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 directly apply 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

⁴² Christopher Kuner, 'Extraterritoriality and regulation of international data transfers in EU data protection law' (2015) 5(4) International Data Privacy Law 235.

⁴³ Anu Bradford, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1.

⁴⁴ Art 23 of the GDPR.

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 European Convention on Fundamental Rights (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 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 (e.g., 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, restricts storage and use of personal data. Article 15 ECHR allows 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 Second, 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 not only been brought before the CJEU but also before the European Court of Human Rights (ECtHR). The ECtHR confirmed in the cases of *Zakharov (2015)* and *Szabo (2016)* 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

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

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

⁴⁷ See C-617/10 *Fransson* and C-206/13 *Siragusa* (n 54)

⁴⁸ Case C-446/12 *Willems* [2015] 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.

⁴⁹ See formulation of question 1:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=en&mode=lst&ir=&occ=first&part=1&cid=6451273>.

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

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

three different surveillance regimes: (1) the bulk interception of communications; (2) intelligence sharing with foreign governments; and (3) 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.

Checks and Balances within the EU

The Court'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 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 the 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 introduces 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.

⁵² *Big Brother Watch and Others v the United Kingdom* App nos 58170/13, 62322/14 and 24960/15.

⁵³ *Centrum för rättvisa v. Sweden* App no 35252/08.

⁵⁴ Art 25(1) DPD.

⁵⁵ Iain Cameron, 'Balancing data protection and law enforcement needs' (n 30).

Concluding Remarks

2018 and 2019 are characterised by increasing geo-economic tensions, such as sanctions, tariffs, FTAs, 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 is likely to be received also as an action that forms part of this growing tension. Data is used not only for law enforcement purposes but is also highly relevant for example for the well-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 is accessed and processed by telecommunication providers (*Tele2*), 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 EU and national citizens. The question remains what is an essentially equivalent level of protection and how can it be ensured in practice? As this is what is necessary in order to justify allowing commercial data transfers on a large scale.

Impunities Surrounding the Deployment of Liaison Officers

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 characterized 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 concerns 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. Their objective is to give effect to and enforce laws of the jurisdiction to which the administrative authority belongs that deploys them (home administration). 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.⁵⁶ 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

⁵⁶ Liaison officers can also be seconded in other policy areas to ease cooperation between administrations, such as in the areas of migration and justice.

are in many cases regarded as a “formal representative” of the sending administration.⁵⁷ They fall outside the EU’s data protection framework described above. Put differently: liaison officers seconded from third countries are exempted from EU data protection standards, including when they act within the EU.

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.⁵⁸ The many challenges stipulated in the Treaties further increasing reflect an international perspective. Over the past two decades cooperation between the EU and third countries has steeply increased.⁵⁹ To that effect, a significant amount of EU secondary law and EU (policy) documents on security and migration⁶⁰ stress the importance of cooperation between competent authorities between the EU and external actors. To establish 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.⁶¹ The objective and tasks for liaison officer secondment focusses on “coordination and cooperation between police and judicial authorities”.⁶² 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 Regulations⁶³, bilateral cooperation agreements⁶⁴, and Memoranda of Understanding⁶⁵ concluded between an

⁵⁷ Art 2(1) Annex 4 agreement on Operational and Strategic Co-operation between the Republic of Colombia and the European Police Office; Art 2 Annex III Agreement on Operational and Strategic Co-operation between the Government of HSH The Sovereign Prince of Monaco and Europol; Art 2 Annex III Agreement between The Republic of Iceland and Europol.

⁵⁸ Art 67(3) TFEU on criminal matters in the Area of Freedom, Security and Justice.

⁵⁹ Jörg Monar, ‘The EU’s growing external role in the AFSJ domain: factors, framework and forms of action’ (2014) 27(1) Cambridge Review of International Affairs 147, 142; Ramses A. Wessel, Luisa Marin, Claudio Matera, ‘The external dimension of the EU’s Area of Freedom, Security and Justice’ in Christina Eckes and Thanos Konstadinides (eds), *Crime Within the Area of Freedom, Security and Justice: A European Public Order* (CUP 2011), 277.

⁶⁰ Council Regulation (EC) 377/2004 of 19 February 2004 on the creation of an Immigration Liaison Officers network [2004] OJ L64/1 (hereafter ILO Regulation), recitals 1, 3 and 4; Art 54 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 (hereafter Frontex Regulation); concluded bilateral agreements between Frontex and third countries: Canada, Turkey and the USA; Chris 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) 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 (hereafter Europol Regulation); Recital 20 Frontex Regulation.

⁶¹ 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; Proposal for a Regulation of the EP and the Council on the creation of a European network of immigration liaison officers COM (2018) 303.

⁶² Herwig C.H. Hofmann, Alexander H. Türk, *EU Administrative Governance*, (Cheltenham, Edward Elgar Publishing, 2006) 343.

⁶³ Art 27(3) 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; Art 12(3) and 54 Frontex Regulation.

⁶⁴ Ibid; ILO Regulation (n 56).

⁶⁵ 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

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 what legal regime implicitly or explicitly applies to the liaison officer, it is therefore 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 to determine what rules and consequent control mechanisms may apply to these liaison officers. A wide array of responsibilities for liaison officers is visible in annual reports of EU AFSJ agencies,⁶⁶ and job vacancies for liaison officers.⁶⁷ The responsibilities vary from far-reaching (i.e. the use of EU and Member State databases for police and migration purposes;⁶⁸ assist and facilitate a swift exchange of information;⁶⁹ support the decision quality of visa decisions⁷⁰) to less far-reaching (i.e. network building;⁷¹ advisory roles⁷²).

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

enhancing cooperation between EU agency and 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, for example, the Annexes to Europol cooperation agreements (n 53).

⁶⁵ Interpol-Europol Memorandum of Understanding; Memorandum of Understanding between Eurojust – United Nations Office on Drugs and Crime (UNODC).

⁶⁶ Europol Review 2016-2017, 64; Frontex, 'A year in review: First 12 months of the European Border and Coast Guard Agency', pp. 3-5.

⁶⁷ E.g. job vacancy for British immigration liaison officers posted 17/05/2016 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.

⁶⁸ Art 8(3), 8(4) Europol Regulation; exchange of information – via liaison officers – via long established channels between EU Member States and third countries; Statewatch website news blog, 'Europol-USA agreement: Was it really needed?' link: <http://www.statewatch.org/news/2006/jul/01europol-usa.htm>.

⁶⁹ 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 [http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategicmeetings/Outcome%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](http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategicmeetings/Outcome%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).

⁷⁰ British immigration liaison officer job vacancy (n 63).

⁷¹ Ersel Aydinli and Hasan Y n, 'Transgovernmentalism Meets Security: Police Liaison Officers, Terrorism, and Statist Transnationalism' (2011) 24(1) Governance: An International Journal of Policy, Administration and Institutions 66, 67.

⁷² Council outcome report, 'Meeting with Eurojust Contact Points and Liaison Magistrates' (n 65).

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).

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, side-lined in that debate. A thorough study of U.S 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 to highlight 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 of public and private parties for law enforcement purposes, liaison officers act as intermediary 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 of which 51 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 they are specified in EU secondary law and the case law of the Court? The following section shows the differences in the selection and deployment procedure of liaison officers seconded by an EU Member State and those seconded by a third country to Europol.

Selection procedure 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 Firstly, 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

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

⁷⁵ M Böse, ‘EU substantive criminal law and jurisdiction clauses: claiming jurisdiction to fight impunity?’, *Fighting Impunities*, *forthcoming*.

⁷⁶ Mariolina Eliantonio, ‘Information exchange in European Administrative law: A Threat to Effective Judicial Protection?’ (2016) 23(3) *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*.

⁷⁹ Europol website <https://www.europol.europa.eu/about-europol/statistics-data>.

⁸⁰ Art 7(3) Europol Regulation, recital 3 Europol Regulation.

⁸¹ Art 8(1) Europol Regulation.

⁸² Art 7 and 8 Europol Regulation.

⁸³ Art 7(2) Europol Regulation.

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. It is, however, the national unit from whom liaison officers receive instructions.⁸⁹ In any case, Member States’ liaison officers are subject to the national law of the designating Member State and remain subject 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, hence, to their own national data protection standards.

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 US 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 question arises what specific parties are involved in these “consultations” as the liaison agreement is still closed from public view⁹⁴ 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, however, a large number of ambiguities related to data protection. The next section shall outline these ambiguities and other spaces in law in which the US liaison officers transfer data to the US

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 US – Europol cooperation agreement allows the exchange of

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.

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, for example the Agreement between the Kingdom of Norway and the European Police Office.

personal data,⁹⁵ despite the fact that the personal data is not protected by EU data protection rules during and after the transfer. The next section sets out the legal structure under which US liaison officers (and other non-EU state liaison officers) operate when seconded to Europol.

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 US with respect to Europol.⁹⁶ Not being members of the Europol staff themselves and subject to their own national laws, US liaison officers for example do not 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 both 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. The Privacy Shield protects in the above-discussed context EU personal data that is transferred to the US 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.

Data protection standards in the supplemental agreements?

As intermediary 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 US and Europol, on the basis of which liaison officers are seconded, are laid down in the supplemental agreement between Europol and the US 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

⁹⁵ www.europol.europa.eu/newsroom/news/today-brazil-and-europol-signed-agreement-to-expand-cooperation-to-combat-cross-border-criminal-activities.

⁹⁶ This is acknowledged in other cooperation agreements: Art 2(1) Annex 4 Colombia – Europol cooperation agreement; Annex to the Moldova – Europol cooperation agreement; Art 2(1) Annex 4 to the cooperation agreement between the Former Yugoslav Republic of Macedonia and Europol (n 53).

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 (hereafter ‘Regulation 2018/1725’).

⁹⁸ Art 2(3) Regulation 2018/1725.

⁹⁹ Art 25(3) Europol Regulation.

¹⁰⁰ Art 2(2)d GDPR.

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.

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 paper, not the same as the European data protection standards.

Conclusions: Impunities from Data Protection?

This paper identified what rules apply to data cooperation with the US in the 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 US and when external officers, that is US liaison officers, are deployed to the EU administration. The paper 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 wide-spread, 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 U.S 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 US remain issues that are approached very differently in the EU and in the US Both issues further are not in the hands of commercial actors. In fact, commercial actors in the US 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 Data Protection Authorities (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.

¹⁰³ Art 7(1) a and b Supplemental Agreement.

¹⁰⁴ Florencia Marotta-Wurgler, ‘Understanding Privacy Policies: Content, Self-Regulation, and Markets’, New York University Law and Economics Working Papers 4-2016, available at: https://lsr.nellco.org/cgi/viewcontent.cgi?article=1439&context=nyu_lewp.

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 US 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.



UNIVERSITY OF AMSTERDAM



AMSTERDAM
CENTRE FOR
EUROPEAN
LAW AND
GOVERNANCE

COMMERCIAL DATA TRANSFERS AND LIAISON OFFICERS: WHAT DATA PROTECTION RULES APPLY IN THE FIGHT AGAINST IMPUNITY WHEN THIRD COUNTRIES ARE INVOLVED?

Christina Eckes

Dominique Barnhoorn

Amsterdam Law School Legal Studies Research Paper No. 2019-42

Amsterdam Centre for European Law and Governance Research Paper No. 2019-04