The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive

Drechsler, Laura

Published in:
Cybercrime: New Threats, New Responses

Publication date:
2020

License:
CC BY-NC-ND

Document Version:
Final published version

Citation for published version (APA):
THE ACHILLES HEEL OF EU DATA PROTECTION IN A LAW ENFORCEMENT CONTEXT: INTERNATIONAL TRANSFERS UNDER APPROPRIATE SAFEGUARDS IN THE LAW ENFORCEMENT DIRECTIVE

Laura Drechsler
Ph.D researcher (FWO aspirant)
FWO, Brussels Privacy Hub, LSTS, VUB

ABSTRACT: In May 2018, EU data protection rules were not only reformed by the General Data Protection Regulation (GDPR) but also by the Law Enforcement Directive (LED). While the LED is often overshadowed by the GDPR, it nevertheless did introduce a number of crucial reforms to data protection in a law enforcement context in the EU including harmonised rules on how personal data in a law enforcement context can be transferred to other law enforcement authorities in third countries. Formally the LED rules on international transfers of personal data to third countries aim at guaranteeing that the level of protection for personal data in a law enforcement context within the EU is not undermined as soon as personal data leaves EU territory. Taking a closer look however reveals major issues with the rules foreseen for transfers in the LED as they often come down to law enforcement authorities self-assessing whether a third country would offer adequate protection within the meaning of the standard of essential equivalence as established by the Court of Justice of the European Union (CJEU) in Schrems.

In this paper, I show, by relying on EU fundamental rights law and the case law of the CJEU, how due to the absence of LED adequacy decisions, personal data transfers to law enforcement authorities in third countries often occur without the appropriate scrutiny and safeguards due to system the LED establishes. Using the recent reference to the CJEU by a German Court regarding information exchanges with Interpol, I demonstrate how the created legal uncertainty can affect both the work of law enforcement authorities and the fundamental rights of individuals. I conclude that the current system for international personal data transfers within the LED is deeply flawed and potentially undermining EU personal data protection in a law enforcement context.

KEYWORDS: Law Enforcement Directive, personal data transfers, standard of essential equivalence, appropriate safeguards, Interpol

1. INTRODUCTION

Due to the borderless nature of the internet on which much personal data ‘moves’ effortlessly and constantly across internal and external borders, the ensuring of the protection
offered by EU data protection law becomes increasingly difficult\textsuperscript{1}. From an EU perspective, the protection of personal data cannot stop at the external borders of the EU, as otherwise circumvention of its rules would undermine the standard of protection for personal data the EU strives to offer\textsuperscript{2}. This standard has been further bolstered by the adoption of the Treaty of Lisbon, which gave the Charter of Fundamental Rights of the European Union (CFR)\textsuperscript{3} the rank of EU primary law, including via the fundamental right to personal data protection of Article 8 CFR.\textsuperscript{4} The interpretation of this right, and other EU fundamental rights at stake when personal data crosses the EU’s external border, by the Court of Justice of the European Union (CJEU) \textit{inter alia} in \textit{Schrems}\textsuperscript{5} confirmed the strong interrelation between EU fundamental rights and the regulation of international personal data transfers\textsuperscript{6}. In \textit{Schrems}, the CJEU has established that in a situation where personal data reaches a third country, the protection for fundamental rights in connection with the processing of such personal data needs to be essentially equivalent to that offered within the EU via the CFR and the secondary data protection instruments (standard of essential equivalence)\textsuperscript{7}.

The strong link between EU fundamental rights and data processing has specific importance in the area of law enforcement, where data processing can assist the investigation and prosecution of criminal offences, but also detrimentally affect the life of the suspect by negating his or her fair trial rights or presumption of innocence\textsuperscript{8}. In May

\begin{itemize}
\item[4] For a history on the emergence of that right, see GONZÁLEZ FUSTER, G. (2014). \textit{The Emergence of Personal Data Protection as a Fundamental Right of the EU}. Springer.
\item[7] CJEU, Case C-362/14 \textit{Schrems}, \textit{supra} note 5, § 73.
\end{itemize}
2018, EU data protection rules were not only reformed by the General Data Protection Regulation (‘GDPR’)\(^9\) but also by the Law Enforcement Directive (‘LED’)\(^10\). While the LED is often overshadowed by the GDPR, it nevertheless did introduce a number of crucial reforms to data protection in a law enforcement context in the EU including harmonised rules on how personal data in a law enforcement context can be transferred to other law enforcement authorities in third countries\(^11\). Formally the LED rules on international transfers of personal data to third countries aim at guaranteeing that the level of protection for personal data in a law enforcement context within the EU is not undermined as soon as personal data leaves EU territory. Taking a closer look however reveals major issues with the rules foreseen for transfers in the LED as they often come down to law enforcement authorities self-assessing whether a third country would offer adequate protection within the meaning of the standard of essential equivalence as established by CJEU in Schrems.\(^12\) A standard declared relevant for the LED in recital 67 LED\(^13\).

In this paper, I show, by relying on EU fundamental rights law and the case law of the CJEU, how due to the absence of LED adequacy decisions, personal data transfers to law enforcement authorities in third countries often occur without the appropriate scrutiny and safeguards due to system the LED establishes. Furthermore, using the recent reference to the CJEU by a German Court regarding information exchanges with


\(^11\)Arts. 35-40 LED.

\(^12\)CJEU, Case C-362/14 Schrems, *supra* note 5, § 73.

\(^13\)The relevance of Schrems for the law enforcement context was also highlighted by the European Data Protection Supervisor (EDPS) and the Article 29 Working Party (WP29). See “A further step towards comprehensive EU data protection - EDPS recommendations on the Directive for data protection in the police and justice sector”. *Opinion 6/2015 of the European Data Protection Supervisor* (28 October 2015), p. 13; “Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences”. *Opinion 01/2016 of the European Data Protection Supervisor* (12 February 2016), p. 6; and “Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data”. *Article 29 Data Protection Working Party* (1 December 2015), WP 233, p. 13.
Interpol\textsuperscript{14}, I demonstrate how the created legal uncertainty can affect both the work of law enforcement authorities, whose work depends on being able to access personal data across borders\textsuperscript{15}, and the fundamental rights of individuals. I conclude that the current system for international personal data transfers within the LED is deeply flawed and potentially undermining EU personal data protection in a law enforcement context.

2. \textbf{THE LED SYSTEM FOR INTERNATIONAL PERSONAL DATA TRANSFERS}

2.1. \textbf{Scope of application of the LED}

Before explaining the system, the LED establishes for international personal data transfers, it is useful to explore the scope of application of the LED. Compared to the scope of the GDPR,\textsuperscript{16} the scope of the LED is more limited\textsuperscript{17}. The LED applies to the processing of personal data by competent law enforcement authorities for the purposes of the “\textit{prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security}”\textsuperscript{18}.

For the purposes of international personal data transfers,\textsuperscript{19} the limited scope of the LED translates into its regime being principally only applicable for exchanges from law enforcement authority to law enforcement authority. Only exceptionally transfers can occur to an individual or other entity if the conditions of Article 39(1) are fulfilled. Article 39 LED is applicable, when a transfer to the law enforcement authority in the third

\textsuperscript{14} CJEU, Case C-505/19, \textit{Bundesrepublik Deutschland} (pending).

\textsuperscript{15} The European Commission (Commission) claims that 85\% of investigation rely on electronic evidence, which often includes personal data, and in 2/3 of these investigations obtaining this evidence includes cooperation with non-EU entities. See “Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters”. \textit{European Commission} (5 February 2019), COM(2019) 70 final, p. 1.


\textsuperscript{17} Art. 2(1) LED. Unlike the GDPR, the LED has no specification regarding the territorial scope, as it only applies to competent authorities, which by definition have to be situated in an EU Member State.

\textsuperscript{18} Art. 1(1) LED.

\textsuperscript{19} There is no definition of data transfers in the LED, for the purposes of this paper the term ‘international personal data transfer’ means that personal data originating from the EU has become accessible from outside of the EU. For more information on the problematic of defining data transfers, see GONZÁLEZ FUSTER, G. (2016), “Un-mapping Personal Data Transfers”. \textit{European Data Protection Law Review} (2016), Vol. 2, pp. 160-168.
country would be ineffective and if there is imminent danger to a person to fall victim to a crime. Due to the exceptional nature of Article 39 LED, principally international personal data transfers under the LED will only occur between an EU law enforcement authority and a law enforcement authority in a third country.

2.2. General conditions for international personal data transfers under the LED

A first speciality of the transfer system established by the LED, is the fact that it foresees five general conditions that have to be fulfilled for every transfer under it. These five conditions are exhaustive and only know limited exceptions.

As a first condition, Article 35(1) LED stipulates that any transfer has to be necessary for the purposes of law enforcement (which are defined in Article 1(1) of the LED). Secondly, whoever receives the personal data needs to be an authority competent for law enforcement purposes that is also the controller in that processing operation. The LED strictly speaking thus only foresees transfers to controllers outside of the EU, not to processors. Thirdly, in case personal data are originating from a different EU Member State than the one undertaking the transfer, the latter has to obtain prior authorisation of the for-


21 Art. 35(1) LED.

22 See rec. 64 LED. These conditions were already formulated in the predecessor of the LED, the Framework Decision. Framework Decision. See “Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters”. Official Journal of the European Union (30 December 2008), L 350/60 (no longer in force), Art. 13(1).

23 Art. 35(1)(a) LED.

24 Art. 35(1)(b) LED. These competent authorities are defined in Art. 3(7) LED.

25 There is a debate whether this was intentional, especially since rec. 64 LED mentions a transfer to processors: ‘Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation’ (emphasis added). However, following a strict interpretation of Art. 35(1)(b) LED transfers to processors cannot occur if one of the conditions is that the recipient needs to be a controller. Such transfers could still take place under the framework of Art. 39 LED, which forms one of the exceptions to the condition established in Art. 35(1)(b) LED. See also SAJFERT, J. and QUINTEL, T. (2020), supra note 20, pp. 19-20.
mer\textsuperscript{26}. Fourthly, each transfer under the LED must be based on one of the three available transfer mechanisms: adequacy decisions, appropriate safeguards or derogations\textsuperscript{27} Finally, if there is an onward transfer of the personal data meaning that the controller in the third country transfers the received personal data further, authorisation of an authority in the Member State that initiated the original transfer abroad needs to be obtained\textsuperscript{28}. Any transfers in the framework of the LED can only occur if all these five conditions are fulfilled\textsuperscript{29}.

2.3. The different transfer mechanisms of the LED

As noted above, transfers under the LED can following the fourth condition only be based on the mechanisms the LED provides\textsuperscript{30}. The available transfer mechanisms are: adequacy decisions, appropriate safeguards, and derogations\textsuperscript{31}.

2.3.1. LED adequacy decisions

LED adequacy decisions are regulated in Article 36 LED. If there is an LED adequacy decision, a transfer would not require any further safeguards though the above outlined five conditions continue to apply. The third country or international organisation receiving the personal data is then considered to protect in an equivalent manner the fundamental rights protected in the LED and the CFR\textsuperscript{32}. LED adequacy decisions are adopted by the Commission, who is also tasked with monitoring adopted decisions

\textsuperscript{26} Art. 35(1)(c) LED. In exceptional cases explained in Art. 35(2) LED, transfers can occur without such authorisation but the authority in the Member State otherwise entitled to give authorisation needs to be informed immediately.

\textsuperscript{27} Art. 35(1)(d) LED. See further Art. 36, Art. 37 and Art. 38 LED.

\textsuperscript{28} Art. 35(1)(e) LED and rec. 65 LED.

\textsuperscript{29} These conditions count among its origins, the Recommendation on processing police data by the Council of Europe. See “Regulating the use of personal data in the police sector”. \textit{Recommendation of the Committee of Ministers to Member States} (17 September 1987), R(87) 15. Though Caruana criticises the LED conditions for being weaker, especially because transfers are not conditional on serious and imminent danger because of serious crime. See \textsc{Caruana, M.} (2017). “The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement”. \textit{International Review of Law, Computers & Technology}, Vol. 33, p. 17.

\textsuperscript{30} Art. 35(1)(d) LED.

\textsuperscript{31} Arts. 36, 37 and 39 LED.

\textsuperscript{32} The assessment of the third country and international organisation is regulated in a similar manner than for GDPR adequacy decisions (compare to Art. 45 GDPR). A third country or international organisation should follow the rule of law, have an appropriate level of protection of human rights, and provide effective remedies for individuals as well as independent supervision of the processing. Sources for this assessment are domestic legislation, practice and international commitments. See Art. 36(2) LED and rec. 67 LED.
and to amend, suspend or repeal them if the level of protection does no longer fulfil the adequate fundamental rights standard\textsuperscript{33}.

In terms of fundamental rights safeguards, LED adequacy decisions could offer significant protection for law enforcement exchanges if the provisions of Article 36 LED are followed strictly and if the standard of essential equivalence established in Schrems is respected. However, currently no such decision exists or is in planning, leading to a situation where this mechanism is not an option for law enforcement transfers in practice\textsuperscript{34}.

\textit{2.3.2. Appropriate safeguards and derogations under the LED}

The second option for transferring personal data in a law enforcement context outside of the EU are appropriate safeguards regulated in Article 37 LED\textsuperscript{35}. The LED distinguishes two types of such safeguards: “legally binding instruments” such as “legally binding bilateral agreements”\textsuperscript{36} or a self-assessment by the law enforcement authorities (as controllers) that there are appropriate safeguards in the third country or the international organisation regarding personal data protection\textsuperscript{37}. In case of such a self-assessment, the controller has to inform the data protection authority (DPA) “about categories of transfers” and provide documentation for the DPA that includes “the date and time of the transfer, information about the receiving competent authority, the justification of the transfer and the personal data transferred”\textsuperscript{38}. Most arrangements in force for law enforcement will now be classified as either one of these options for appropriate safeguards, depending on whether the arrangement represents a legally binding instrument\textsuperscript{39}. In absence of appropriate safeguards, the LED foresees a number of derogations listed in Article 38 LED,

\textsuperscript{33} Art. 36(3),(4),(5) and (6) LED.

\textsuperscript{34} In its latest public statement on LED adequacy decisions of July 2019, the Commission stated that it would assess the possibilities for LED adequacy decisions to further the cooperation ‘\textit{with key partners in the fight against crime and terrorism}’. No key partner was concretely named, nor is there any official information of any negotiations for LED adequacy in planning. See “Data Protection rules as a trust-enabler in the EU and beyond - taking stock”. \textit{Communication from the Commission to the European Parliament and the Council} (24 July 2019), COM(2019) 374 final, p. 13.

\textsuperscript{35} Art. 37(1) LED.

\textsuperscript{36} Art. 37(1)(a) LED and rec. 72 LED.

\textsuperscript{37} Art. 37(1)(b) LED.

\textsuperscript{38} Art. 37 (2) and (3) LED.

\textsuperscript{39} The current arrangement for law enforcement exchanges with the US, the Umbrella Agreement, would be considered a binding and enforceable instrument, hence be classified under Art. 37(1)(a) LED. See “Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences”. \textit{Official Journal of the European Union} (10 December 2016), L 336/3; “Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Direc-
that can be relied upon by the law enforcement authority unless the transfer would detrimentally affect the fundamental rights of the concerned data subjects\textsuperscript{40}.

Unlike in the GDPR, where nearly all options for appropriate safeguards except for international agreements require authorisation of either the Commission or the DPA\textsuperscript{41}, the LED does not foresee such regulatory oversight. Moreover, while the GDPR lists concrete legal instruments that can be used as appropriate safeguards\textsuperscript{42}, the LED gives no detail on what exactly such appropriate safeguards are\textsuperscript{43}. Due to the absence of LED adequacy decisions and because the derogations for transfers are not always applicable, appropriate safeguards under Article 37 LED are currently the only truly available option for law enforcement cooperation with third countries from an EU perspective. As the next section will demonstrate, this is rather problematic from the perspective of fundamental rights.

### 3. APPROPRIATE SAFEGUARDS UNDER THE LED AND EU FUNDAMENTAL RIGHTS

As described above, appropriate safeguards under Article 37 LED are currently the most likely option for EU law enforcement authorities to cooperate with their counterparts outside of the EU due to the absence of LED adequacy decisions. Both of the options for appropriate safeguards (legally binding agreements and self-assessed safeguards) show significant issues from the perspective of EU fundamental rights.

\textsuperscript{40} Art. 38(2) LED. Derogations include the protection of vital interests of the data subject and the prevention of an immediate and dangerous threat to public security (Art. 38(1)(a) and (c) LED).

\textsuperscript{41} Compare to Art. 46-47 GDPR.

\textsuperscript{42} For a comparison, in the GDPR available appropriate safeguards are listed in Art. 46(2) GDPR and include international agreements between public authorities, binding corporate rules, (standard) contractual clauses, code of conducts, certification mechanisms and administrative arrangements for public authorities.

3.1. Legally binding agreements

In the case of “legally binding agreements”, EU fundamental rights issues stem from the fact that existing agreements in the area of law enforcement are not holding up to the standard of essential equivalence regarding their protection of fundamental rights, also because they were often put in place long before this standard was established. For law enforcement personal data, there are a myriad of these already existing agreements by the EU and Member States with third countries, with often little regard to EU fundamental rights. According to Article 61 LED these previous agreements remain in force “until amended, replaced or revoked”. This is especially a problem with mutual legal assistance treaties (MLATs), which are the traditional instrument for international law enforcement cooperation.

For example, the MLAT with the United States (US) was supplemented by the Umbrella Agreement to improve the protection of fundamental rights. In the system of the LED, the Umbrella Agreement is considered an appropriate safeguard under Article 37(1)(a) LED, as a binding and enforceable instrument. In July 2019, the Commission announced that the Umbrella Agreement could even serve ‘as a model for similar agreements with other important security partners’. However, there are several reasons to doubt the compliance of the Umbrella Agreement with the EU fundamental rights standard for data transfers. First of all, the Umbrella Agreement does not

---


They are often non-compliant with EU fundamental rights, as has been demonstrated for example for the EU MLATs for the US and Japan in a study by Fondazione Giacomo Brodolini. See “Fundamental rights review of EU data collection instruments and programmes”. Fondazione Giacomo Brodolini (2019), pp. 55-61.


According to the Commission, the Umbrella Agreement ‘retroactively’ solved data protection issues, that law enforcement transfers had to the US. See ”Minutes of the ninth meeting”, supra note 39, p. 2.


Criticism on the Umbrella Agreement has also come from both the EDPS and the European Data Protection Board (EDPB). See “Preliminary Opinion on the agreement”, supra note 13, p. 17; “LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection”. European Data Protection Board and European Data Protection Supervisor (10 July 2019), pp. 1-2.
include any details or assessment of the US legal system for law enforcement data, but lists a set of principles that both the US and the EU are assumed to have implemented\textsuperscript{51}. Whether these principles are actually put in place in a manner protective of EU fundamental rights is not assessed\textsuperscript{52}. This leads to the second issue, namely, that there are known problems with the US system for law enforcement personal data, that were at the core of the case in \textit{Schrems}, such as unfettered access to personal data by US intelligence agencies, or a lack of clarity on effective remedies for an EU citizen in front of US courts\textsuperscript{53}. It is not clear whether the Umbrella Agreement safeguards from any of these problems.

Should new legally binding instruments be negotiated, they would have to also obtain the standard of essential equivalence regarding the protection of EU fundamental rights and thus improve the fundamental rights protection of this appropriate safeguard. However, it is not clear whether there are any incentives for either the EU or the Member States to negotiate new agreements, considering the continuing validity of the old arrangements under Article 61 LED and the complexities involved in negotiating an agreement in this area. From the perspective of EU fundamental rights, this leads to the unsatisfactory outcome that personal data are transferred for law enforcement purposes outside of the EU without the required fundamental rights guarantees, thus creating the first part of the Achilles heel in the protection of fundamental rights within the context of personal data processing for law enforcement purposes.

\subsection{3.2. Self-assessed appropriate safeguards}

The second option for appropriate safeguards—self-assessed safeguards, does not fare better than binding agreements from an EU fundamental rights perspective. Within this option, a law enforcement authority has to assess itself, whether its partner in a law enforcement cooperation provides a level of EU fundamental rights protection linked to the processing of personal data that is essentially equivalent to the EU\textsuperscript{54}. It thus puts the

\begin{itemize}
  \item \textsuperscript{51} “Agreement”, \textit{supra} note 39, Art. 1.
  \item \textsuperscript{52} A first joint review of the Umbrella Agreement has to take place no later than three years from entry into force of the agreement, which should have been December 2019 the latest. It will be interesting to see if the review will finally an assess whether the US actively implemented all the principles. Ibid., Art. 23(2).
  \item \textsuperscript{53} CJEU, Case C-362/14 \textit{Schrems}, \textit{supra} note 5. While the Commission tried to address these issues in the Privacy Shield, the recent Opinion of the Advocate General (AG) in \textit{Schrems II} makes it doubtful that this was successful. See ADVOCATE GENERAL SAUGMANDSGAARD Æ, Opinion in Case C-311/18. \textit{Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems} (2019). ECLI:EU:C:2019:1145, §§ 196-342.
  \item \textsuperscript{54} Following the AG in \textit{Schrems II}, I argue that all transfer mechanism in EU data protection law have to fulfil this standard, hence also self-assessed appropriate safeguards. See ibid., § 117.
\end{itemize}
significant burden of securing EU fundamental rights on the shoulders of law enforcement authorities, who have neither the legal expertise nor the resources to deal with such complicated matters. In addition, law enforcement authorities will have to conduct this assessment without guidance by either the EDPB or their national DPA, as both have so far been inactive concerning issues of the LED\textsuperscript{55}.

While technically, a law enforcement authority could properly assess a partner under the standard of essential equivalences, changes of getting it right are stoked against them, considering the continuous flaws that are pointed out in the assessments of the Commission, who have more expertise and time to deal with them\textsuperscript{56}. A law enforcement authority under pressure to conclude an investigation should not be put under the additional strain of having to solve complex fundamental rights law issues linked to international personal data transfers\textsuperscript{57}. The below preliminary reference to the CJEU (Case C-505/19) concerned with such self-assessed appropriate safeguards further illustrate the complexity of the legal issues a law enforcement authority would have to address and the madness of the EU legislator to “dump” this important task on national law enforcement authorities.

4. THE PRELIMINARY REFERENCE C-505/19: INTERNATIONAL PERSONAL DATA TRANSFERS TO INTERPOL

4.1. Case C-505/19 Bundesrepublik Deutschland

The case resulting in the preliminary reference Case C-505/19\textsuperscript{58} concerned the request for deletion by a former manager of a big Germany company (‘the applicant’), who had been investigated for bribery in relation to business transactions with an Argentine firm between 2002 and 2007 by the Munich public prosecutor, of a red

---

\textsuperscript{55} The EDPB Website section for guidance on the LED is so far completely empty (status: January 2020). As far as I could see, there is not much guidance by national DPAs either. Anecdotes suggest that national DPAs also currently lack expertise to deal with issues linked to the LED, and are fighting with the general issues of being under-resourced and under-staffed.

\textsuperscript{56} The CJEU has reversed the assessment made by the Commission in Schrems and Opinion/15. See CJEU, Case C-362/14 Schrems, supra note 5, §§ 79-98; and CJEU, Opinion 1/15. Opinion pursuant to Article 218(11) TFEU. ECLI:EU:C:2017:592, § 232. If it rules on the validity of the Privacy Shield in Schrems II and follows the argumentation of the AG, another failed assessment would be added to this list. See ADVOCATE GENERAL SAUGMANDSGAARD ØE, supra note 53, §§ 196-342.

\textsuperscript{57} CARUANA (2017), supra note 29, p. 17.

\textsuperscript{58} CJEU, Case C-505/19, Bundesrepublik Deutschland, supra note 14.
alert issued via the Interpol system\(^59\). These German proceedings had ended with the applicant paying a monetary compensation. The request for the deletion of the red alert was placed with the German Federal Criminal Police Office (“Bundeskriminalamt”), who are the central contact point (‘national bureau’) between Interpol and the German police\(^60\), and subsequently ended in front of the administrative court of Wiesbaden (‘the referring court’). The red alert the applicant wanted to delete stemmed from the US, where public prosecution had also started to investigate the applicant for fraud relating to the same business transaction. This red alert continued to show in the Interpol system, despite Germany informing Interpol that the matter had been handled by the German justice system and that the red alert was running counter to the prohibition of double-jeopardy (“\textit{ne bis in idem}”) \textit{inter alia} enshrined in Article 50 CFR. Interpol claimed that they could not delete the red alert as only the state that issued it can do so. As a consequence of this red alert every state member of Interpol (among them all the EU Member States) would be under pressure to arrest the applicant if he entered their territory\(^61\).

Against this background, the referring court posed two sets of questions to the CJEU: On the one hand they inquired about the relation between the prohibition of double-jeopardy enshrined in Article 50 CFR, freedom of movement of EU citizens secured in Article 21(1) TFEU and the Interpol red alert system\(^62\). On the other hand, they questioned whether the data processing that was inherent in the implementation\(^59\)

---

\(^59\) Red alerts are requests to arrest a certain individual. While they are not technically a legal arrest warrant as they are not binding, they do in practice serve that purpose due to high compliance by the Member States of Interpol, as illustrated by Savino. See SAVINO, M. (2011). “Global Administrative Law Meets Soft Power: The Uncomfortable Case of Interpol Red Notices”. \textit{N.Y.U Journal of International Law and Politics}, Vol. 43, p. 298.

\(^60\) For a summary of the facts, see “Verwaltungsgericht Wiesbaden legt EuGH Fragen zu Interpol vor”. \textit{Verwaltungsgericht Wiesbaden} (3 July 2019), Presseinformation.


\(^62\) “Case C-505/19, Request for a preliminary ruling”, supra note 61, pp. 2-3 (questions a, b, c, f). The referring court wanted to know \textit{inter alia} whether the prohibition of double-criminality applied in the case at hand, where investigations ended with the payment of a monetary payment by the accused, and whether an EU Member State was obliged to refuse the implementation of a red alert coming from Interpol if another EU Member State issued concerns about its compatibility with the prohibition of double-criminality.
of a red alert from Interpol was actually in line with the LED, especially the transfers from Interpol to the Member States\textsuperscript{63}. These two sets of questions are linked: if the prohibition of double-jeopardy applies in this context (and the referring court seems to be convinced it does), the red alert would counter EU fundamental rights which could pose an issue with the principle of lawfulness at the basis of the LED\textsuperscript{64}.

4.2. Potential consequences of the preliminary reference for international personal data transfers under the LED

In its second set of questions, the referring court is essentially asking whether Interpol has an adequate level of personal data protection for the purposes of the LED personal data transfer system. In other words, the referring court is inquiring whether the arrangement for personal data protection at Interpol offers enough protection for the German Federal Criminal Police Office to self-assess it positively. Answers to these questions would provide essential guidance on how to conduct such a self-assessment and clarify the legal basis for exchanges with Interpol. Unfortunately, there is a possibility that the CJEU will not find answering these questions relevant for the resolution of the reference due to the first set of questions. If the CJEU finds the prohibition of double-jeopardy protected \textit{inter alia} in Article 50 CFR interfered with and if it finds, as the referring court suggests, that such an interference also negates any lawfulness of the processing following Article 8 LED (because the legal basis for the processing – the red alert – would then be violating EU fundamental rights, and is thus unsuitable as a legal basis), the case could be solved without answering the questions concerning personal data transfers, as the processing is already unlawful.

In case the CJEU does answer the questions on whether the Interpol data processing regime offers enough protection from the perspective of Article 37(1)(b) LED, it is hard to predict what it would find. The exchange of personal data with Interpol is a primary example for the issues pointed out in this paper. There is no adequacy decision for Interpol\textsuperscript{65}, hence exchanges would have to rely on either legally binding agreements or self-assessed appropriate safeguards. While there is one aspect at EU level that resembles a more binding arrangement for exchanges with Interpol – the exchange of

\textsuperscript{63} \textit{Ibid.}, pp. 2-3 (questions d and e).

\textsuperscript{64} \textit{Ibid.}, pp. 7-8. See also Art. 4(a) and Art. 8 LED.

\textsuperscript{65} This is a novelty of the LED, which introduced the option to adapt adequacy decisions for international organisations. See Art. 36(1) LED. Whether Interpol is actually an international organisation is a question in itself, outside the scope of this paper, though Savino is convincing in his argument that Interpol is at least an international organisation according to customary public international law. See SAVINO, M. (2011), supra note 59, pp. 271-272.
information concerning “issued and blank stolen, lost or misappropriated passports”66 – the scope of this is limited to information about passports and does not include red alerts67. On a national level, there might be agreements between the national police bodies and Interpol68 but for the Commission these do not suffice as a legal basis for data transfers, and therefore these exchanges should be based on Article 37(1)(b) LED (self-assessed appropriate safeguards)69.

Unlike for other such self-assessments, the LED itself provides a recital on how transfers to Interpol should be considered70. Specifically, recital 25 LED clarifies that for international personal data transfers to Interpol, the LED and its provisions for such transfers apply71. As guidance for law enforcement authorities, this is however only helpful to a very limited extent. That the EU legislator did not consider the relationship with more details is a pity, as the personal data protection of Interpol seems lacking from an EU fundamental rights perspective. Digging into that regime, reveals holes in the protection of the rights of the individuals due to a lack of effective remedies72 (an issue found highly problematic by the CJEU in Schrems73). Additionally, oversight of Interpol is not guaranteed in the independent manner required by EU data protection law, as the structure of the Commission on the Control of Interpol’s File (CCF)– Interpol’s over-


67 Such exchanges can only occur if the shared personal data ‘shall only be accessible to members of Interpol from countries that ensure an adequate level of protection of personal data’. See ibid., Art. 55(2).

68 According to Interpol’s rules on the processing of data (IRDP), every member organisation to Interpol has to include in the agreement with Interpol the acceptance of the IRDP. See “INTERPOL’s Rules on the Processing of Data”. Interpol (2019) III/IRPD/GA/2011 (2019), Art. 21(3).


70 Rec. 25 LED.

71 Ibid.

72 Interpol foresees the rights of access, erasure and rectification. Decisions on these rights are however only binding on Interpol itself, they cannot help in a case, like the one at issue, where the fundamental rights problem stems from the origins of the red alert, if the state issuing the red alert, is refusing to take action. Therefore, remedies lack effectiveness. See Art. 18(1) IRPD; and “Statute of the Commission for the Control of INTERPOL’s Files”. Commission for the Control of Interpol’s Files (11 March 2017) II.E/RCIA/GA/2016, Arts. 29-32. For an explanation of the Interpol’s data processing system before the reform in 2016 and its flaws, see WUI LING, C. (2010). “Mapping Interpol’s Evolution: Function Expansion and the Move to Legalization”. Policing, Vol. 4, pp. 36-37.

73 CJEU, Case C-362/14 Schrems, supra note 5, § 95.
sight body for personal data processing — reveals serious flaws. For example, the CCF is both advisor for personal data protection *ex ante* for all matters concerning personal data protection of Interpol, as well as oversight authority in two instances *ex post*, leading to the frequent assessment of its own advice. Against this background, it is not surprising that the referring court voiced doubts on the compatibility of the Interpol data protection regime with the LED.

Considering the importance of Interpol for EU police forces, the case will also be decided in a politically charged environment, making predictions even more unreliable. It is clear though, that the CJEU will have to struggle with many issues pointed out in this paper, above all the difficult question how to assess the data protection regime of a third country with the limited resources of a federal police office according to a EU fundamental rights standard that so far even the Commission never achieved in practice (at least whenever it was tested in front of the CJEU, the Commission’s assessment was found lacking).

5. CONCLUSIONS

Due to the absence of LED adequacy decisions, non-compliant international and bilateral binding agreements and self-assessed appropriate safeguards are currently the only available options for authorising an international personal data transfer to a law enforcement authority outside of the EU. As pointed out in this paper, both of these options are weak in regard to the protection of EU fundamental rights, representing an Achilles heel of the EU data protection regime for law enforcement in two ways.

On the one hand, the lack of fundamental rights protection creates a weakness in the protection of EU individuals in an area where the processing of personal data can have especially severe consequences for the individual, as it can for example lead to their unjustified arrest (e.g. in case of a red notice). On the other hand, the legal uncertainty created by the LED system for data transfers with its heavy reliance on EU law enforcement authorities to protect fundamental rights without guidance by the data protection institutions, risks hampering international cooperation in law enforcement, and thus the effective investigation and prosecution of crimes that also affect EU fundamental.

74 “Statute of the Commission for the Control of INTERPOL’s Files”, *supra* note 72, Art. 3. The lack of independence has been found in need of reform by the Parliamentary Assembly of the Council of Europe. See “Abusive recourse to the Interpol system”, *supra* note 61, p. 2; and “Interpol reform and extradition proceedings”, *supra* note 8, p. 3.

75 See on the political context of red notices themselves, LEMON, E. (2018), *supra* note 61.

76 See CJEU, Case C-362/14 Schrems, *supra* note 5, §§ 79-98; and CJEU, Opinion 1/15, § 232.
rights. The practical relevance of the issues pointed out in this paper is confirmed by the preliminary reference Case C-505/19 probing the suitability of the LED data transfer system for exchanges with one of the most important international law enforcement cooperation enabler - Interpol. It is now up to the CJEU to bring with its decision some much needed clarity into the complex area of international law enforcement personal data transfers.

BIBLIOGRAPHY


CJEU, Case C-505/19, Bundesrepublik Deutschland (pending).


“LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection”. *European Data Protection Board and European Data Protection Supervisor* (10 July 2019).


“Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data”. *Article 29 Data Protection Working Party* (1 December 2015), WP 233.


“Regulating the use of personal data in the police sector”. *Recommendation of the Committee of Ministers to Member States* (17 September 1987), R(87) 15.


