ADiM BLOG
June 2021
ANALYSES & OPINIONS

Privacy enhancing readmission: the clause on data protection in the EURAs[1]

Francesca Tassinari

Ph. D. candidate in Public International Law and International Relations
University of Granada[2]

Key Words

Data transfer – Privacy – Irregular migrant – EURAs' clause – Enforceability

Abstract

The identification of third country nationals (TCNs) enables the implementation of the European Union (EU) policy on the prevention of illegal entry and the expulsion of irregular migrants. Competent authorities exchange personal data to prove the nationality and to meet the conditions required to execute the return of TCNs. The EU readmission agreements (EURAs) are provided with a clause regulating the transfer of personal data and its protection. The current post analyses the conformity of the EURAs' clause in the light of the guarantees enshrined in the latest data protection package adopted under the aegis of the EU competence on the protection of personal data and their free movement, namely Article 16(2) of the Treaty on the Functioning of the EU (TFEU). The purpose is to assess whether the EURAs' clause integrates the parameters of "appropriate safeguard" required by Article 46 of the General Data Protection Regulation (GDPR).

[1] I am extremely grateful to Prof. Fajardo del Castillo for her constant guidance in my Ph. D. studies, one more time for her support in the writing of the current post. Any mistakes remain at my expense.
[2] The thesis is co-supervised by Prof. Serena Forlati of the University of Ferrara to whom I extend my sincere thanks for fostering my vocation and academic education.

1. Introduction

Since the 90s, the European Union (EU) has been building up a model system based on the protection of personal data that balances the need of exchanging the information with the provision of specific guarantees preventing unlawful processing of personal data or effective readdress in case of breach. For this reason, EU readmission agreements (EURAs) have been fitted with a data protection clause that imposes the respect of continental parameters on the contracting party. However, the EURAs' clause is not directed at guaranteeing enforceable rights to individuals which raises serious concerns on the effective protection of migrants' fundamental rights to privacy and to the protection of personal data – Articles 7 and 8 of the Niece Charter (CFREU). This circumstance raises uncertainties on whether the EURAs' clause *per se* constitutes an "appropriate safeguard" in terms of Article 46 of the General Data Protection Regulation (GDPR) as it is assumed, e.g., by Article 41(2)(b) of the Entry/Exit System (EES) Regulation.

2. The EU competence on the protection of personal data and their free movement

The EU competence on the protection of personal data had been developed by virtue of Article 100a Treaty of the European Community (TEC) and it was inserted within the provisions having general application of the TFEU by the Lisbon Treaty in 2007. Despite its strategic position, Article 16(2) TFEU suffers from a turbulent history that still influences its exercise: first, it assumes different shapes in specific policies – e.g., in the Police and Judicial Cooperation in Criminal Matters (PJCCM) – because of its sectorial origin; second, it maintains an intimate relationship with the right to privacy set forth in Human Rights Treaties like the European Convention on Human Rights (ECHR) and, today, the fundamental right to the protection of personal data sealed in the CFREU.

These peculiarities harshen the assessment on the existence and nature of the EU external competence on personal data for which purpose the regime on the transfer of personal data set forth in Title V of EU *acquis* on personal data – namely the GDPR and the Data Protection Directive for Law Enforcement (DPDLE) – acquires special relevance. First of all, the existence of the EU external competence has to be inferred by virtue of the *ERTA* doctrine on implied external competences. In this regard, Article 16(2) TFEU suggests that the EU shall pursue two main objectives: the protection of individuals with regard to the processing of personal data as well as to their free movement. The necessity of the EU intervention to act externally is firstly justified by the need to ensure the non-circumvention of EU standards in transborder data flows. This goal is reached, first of all, with the adoption of an adequacy decision (Article 45 GDPR), that is, an implementing decision adopted by the European Commission establishing that a third country or international organisation ensures

a level of protection essentially equivalent to the one granted by the EU. In case there is not a similar decision – or when this has been annulled – the EU is empowered to conclude an international agreement based on Article 16(2) TFEU. Yet, the GDPR does not fully harmonise the data protection field as "(…) there is still a degree of fragmentation which is notably due to the extensive use of facultative specification clauses" – e.g., as far as the age of children consent is concerned (Article 8 GDPR). This situation leads Hijmans to maintain that "the fundamental rights of privacy and data protection on the internet cannot be achieved by internal rules [so that] the effectiveness or *effet utile* of the internal regulation justifies exclusive competence for external action".

As Kuner highlights, the relationship between adequacy decisions and international treaties remains somehow unclear. In *Opinion 1/15* the Court of Justice of the EU (CJEU) maintained that the EU-Canada transborder flow of Passenger Name Record (PNR) should have been based on an agreement or an adequacy decision, alternatively. However, the GDPR clearly places international agreements in a separate layer, within the appropriate safeguards, and under the "legally binding and enforceable agreement" label (Article 46(2)(a) GDPR). In *Maximillian Schrems* the CJEU specified that, differently from adequacy decisions, standard contractual clauses (Article 46(2)(c) GDPR) may require the adoption of supplementary measures and, in any case, their adoption leaves the data controller or processor accountable for supervising the recipient's compliance with the standards agreed. Specifically, Article 46(1) GDPR recalls that the agreement must include enforceable data subject's rights and effective legal remedies so that the foreign country is pushed to comply with its obligations by other contracting parties as well as by the individual. These additional guarantees lead to conclude that the adequacy decision and the corresponding treaty shall be kept separate from each other, though the former may be prodromic to the conclusion of the latter. Besides, a dividing line must be traced between those treaties genuinely concluded on the basis of Article 16(2) TFEU – e.g., the EU-US Umbrella Agreement – and those that contemplate it as a sided legal basis – e.g., the draft EU-Canada PNR Agreement – and, lastly, those that merely foresee a data protection clause, as it is the case of EURAs.

3. Third countries of origin and transit's commitment to privacy and data protection

As of today, the EU has concluded seventeen EURAs. All EURAs include a data protection clause through which the EU promotes its model system in conformity with the parameters set forth in its internal legislation. However, the commitment of third countries of origin and transit *vis-à-vis* privacy and protection of personal data of migrants readmitted varies considerably. Although none of the third countries at issue has been granted an EU adequacy decision, thirteen of them take part in the Council of Europe's Convention No 108.

Convention No 108 is the only legally binding multilateral agreement in the field of

data protection and its provisions are so close to the EU ones that its accession facilitates the adoption of an adequacy finding by the European Commission (recital (105) GDPR). Besides, the European Commission elucidates that Convention No 108 contains safeguards similar to the EU ones, so that the adherence to it ensures a higher level of protection and facilitates the exchange of data on the basis of appropriate safeguards, including public international law (PIL) treaties. Convention No 108 will be provided of an own regime on the transborder flow of personal data among contracting parties as soon as the second amending Protocol will enter into force. Although its Article 14(1) prohibits hampering the transfer of personal data, Convention No 108+ will make exception in case of "(…) harmonised rules of protection shared by States belonging to a regional international organisation". Such a compatibility clause has been specifically inserted to allow Member States to comply with both the Convention No 108+ and Chapter V GDPR since the ratification of Convention No 108+ is not sufficient to meet the EU standards.

4. The clause on data protection in EURAs

The EURAs' clause is made of two main parts, namely an introductory *chapeau* and a set of core principles. Provided that the term "transfer of personal data" used under the EU legislation has not been defined, it can be argued that this concept includes what the EURAs' clause describes as "communication" of data. The EURAs' clause indicates that data are transferred between "competent authorities" of the third country and the Member States – e.g., excluding EU agencies. However, these officials are laid down in unpublished implementing Protocols and it is not possible to know *a priori* which categories of authorities are accountable for the processing of personal data. Conversely, the data subject should be informed of the identity and contact details of the controller according to Articles 13(1)(a) and 14(1)(a) GDPR in order to raise an appeal against them (Article 79 GDPR). Besides, no definition of "processing" is given, and it is not clear how it differs from the expression "treatment of personal data". The applicable laws to the processing of personal data are, respectively, the foreign one in the third country and the Member State's one in the EU, having been the latter harmonised by the Data protection Directive (DPD). Since the GDPR establishes the maximum level of protection, the reference to the Member State's internal legislation should be replaced by a new one to the GDPR.

In its body, the EURAs' clause lists a set of norms that recalls numerous data protection principles which shall be welcomed with favour; yet, still some criticism can be raised. First, by recalling two of the essential elements listed by Article 8(2) CFREU, the clause states that personal data must be processed fairly and lawfully (Article 5(1)(a) GDPR). Second, it sets forth that personal data must be collected for the specified, explicit, and legitimate purpose of implementing the EURA and not further processed by the

communicating authority or by the receiving authority in a way incompatible with that purpose (Article 5(1)(b) GDPR). The principle of purpose limitation is a milestone of the fundamental right to the protection of personal data, but it is not absolute. In the frame of transborder flow of data it may be advisable to oblige the parties to authorise each other to process personal data for further compatible purposes within the limits enshrined in Article 6(4) GDPR.

Third, personal data must be adequate, relevant, and not excessive in relation to the purpose for which they are collected and further processed (Article 5(1)(c) GDPR). Although not embedded in Article 8 CFREU, the principle of data minimisation integrates the strict necessity test deployed under Article 52(1) CFREU and is a crucial feature for assessing the legality of the transfer operation. Concretely, the categories of data communicated shall be specified, and so do the EURAs' clause and the lists annexed to the agreements. The same rationale underpinning the purpose limitation principle applies to storage limitation. The clause states that personal data must be kept in a form which permits identification of data subjects for no longer than what is necessary for the purpose for which the data were collected or for which they are further processed (Article 5(1)(e) GDPR). However, the specification of a maximum data retention period would fulfil the requisite of Article 52(1) CFREU.

Fourth, the EURAs' clause foresees that data shall be kept accurate and, where necessary, up-to-date (Article 5(1)(d) GDPR) which justifies the right to access and rectification recognised to individuals by the CFREU too. Hence, the clause maintains that both the communicating authority and the receiving authority shall take every reasonable step to ensure, as appropriate, the rectification, erasure, or blocking of personal data where the processing does not comply with the provisions of such Article. This provision is particularly relevant in case data are not adequate, relevant, accurate, or they are excessive in relation to the purpose of processing (Articles 16-18 GDPR). Besides, the EURAs' clause establishes that competent authorities shall notify any rectification, erasure, or blocking to the other contracting party, which is consistent with the European Data Protection Board (EDPB) indications.

Some duties on the principle of confidentiality and security of data can be extracted from the restriction of the communication of personal data to the competent authorities only (Article 5(1)(f) GDPR), while imposing the prior consent of the communicating authority in case further communications are made to other bodies. This rule acquires an added value with regard to the so-called "onward transfer" that shall be subject to the same principles and safeguards valid for the first transfer with due respect of the purpose limitation principle. "Onward transfers" shall be subject to the prior and express authorisation of the transferring body and should be recorded and made available to the data protection authority (DPA) if necessary. In this regard, the wording used by the EURAs' clause should

be more trenchant in extending the reach of the EU protection to other recipients. Besides, no explicit mention is made of the principle of security and the need to cooperate in case of data breach. Article 4(12) GDPR obliges to inform the data subject of the high risks stemming from a data breach, including when this is the result of a security incident (Article 34 GDPR). Finally, although we positively welcome the insertion of a binding disposition on the communicating and the receiving authorities to keep a written record of the communication and receipt of personal data (Article 5(2) GDPR), the principle of accountability might have been enhanced by requiring the submission of such a reporting activity to the DPA.

Further safeguards may be added, like the prohibitions of decisions fully based on automated-decision making and of transferring "special categories of personal data" (Article 9 GDPR). The EURAs rely on biometrics to identify individuals which derogates to the general prohibition set forth by the GDPR. Hence, enhanced safeguards should be added like, for example, the insurance that experts are involved in the enrolment phase. Finally, it is not clear why the EURAs' clause affirms that "upon request, the receiving authority shall inform the communicating authority of the use of the communicated data and of the results obtained therefrom". If the data shall be used for the purposes of readmitting migrants to the State of origin or transit only, why should the receiving authority not communicate the result of the use of the communicated data?

5. The enforceability of data subject rights and effective legal remedies

Article 46(1) GDPR demands the controller or processor in charge of transferring personal data on the basis of appropriate safeguards to assess whether "enforceable data subject rights and effective legal remedies for data subjects are available". In international treaty law, enforceability firstly refers to the regulator who must give effect to the data protection dispositions through the implementation of the agreement at issue. PIL instruments – be they hard/soft or punitive/incentive – induce the contracting parties to comply with their commitment. In bilateral relations, and in case the parties of the agreement do not resolve the dispute friendly, they should suspend or terminate the treaty. Article 60(3)(b) of the Vienna Convention on the law of treaties (VC69) requires the violation to be an essential provision "to the accomplishment of the object or purposes of the treaty" unless the parties have agreed otherwise. The EDPB also suggests that in such a circumstance the data transferred shall be returned or deleted by the receiving authority, and the DPA shall be notified.

In the data protection field, the EU promotes "enforceability" through bottom-up mechanisms too. First, DPAs are called to ensure the compliance with data protection principles, including those agreed internationally. Hence, the oversight authority of the receiving State should be called to cooperate with EU DPAs. Second, the data subject must

be recognised the access to redress mechanisms in case foreign authorities do not comply with the agreed provisions. Indeed, the GDPR guarantees not only the right to a judicial remedy in full respect of Article 47 CFREU, but also the right to a compensation in case of damage (Article 82 GDPR). If a judicial remedy is not guaranteed, the EDPB recommends ensuring the availability of alternative safeguards – e.g., arbitration, alternative dispute resolution, or mechanisms implemented by international organisations.

Regrettably, the EURAs' clause does not foresee any provision, neither on DPAs nor on the enforceability of the rights recognised to the data subject. Although the clause requires the communicating and the receiving authorities to take every reasonable step to ensure, as appropriate, the rectification, erasure, or blocking of personal data where the processing does not comply with the agreement, it does not empower the individual *vis-à-vis* public authorities. Conversely, the principle of transparency enables the data subject to take knowledge of: the personal data processing activities public authorities carry out with their data; the relevant tools used for the transfer; the entities to which the data may be transferred; the rights available and the applicable restrictions; the existence of available redress mechanisms, and the contact details for submitting a dispute or claim. However, the allowance of restrictions shall be laid down in accordance with Article 23 GDPR in order to limit the restrictions applicable to the individuals' rights. Therefore, the EDPB urges the contracting parties to publish the agreement and provide a summary thereof in case this facilitates its clarity.

All in all, the EURAs' clause does not comply *per se* with Article 46(1) GDPR requisites unless further guarantees are set forth in the unpublished implementing Protocols mentioned *supra*, which is not known to us. Another option would be to confer direct effect to the EURAs' clause by affirming its clear, precise, and unconditional wording. However, the necessity of its subsequent development through implementing arrangements is heading in the opposite direction. Despite this, Article 98 GDPR confers great discretion – more than the one envisaged by Article 62(6) DPDLE – on the EU legislator when it comes to revising existing EU acts, including international agreements. Recital (102) GDPR establishes that the Regulation "(…) is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects". If treaties previously concluded by the EU that imply the transfer of personal data have not to be amended in the light of the GDPR, it means that they still govern the transfer of personal data in the lack of an adequacy decision.

6. Conclusion

The EURAs are provided with a data protection clause through which the EU promotes its data protection principles. As such, this clause does not provide for

"appropriate safeguards" in terms of Article 46 GDPR. The GDPR does not require that the instrument with which data are transferred has these characteristics, yet it imposes to the controller or processor to assess the availability of "enforceable data subject rights and effective legal remedies". A systemic interpretation of existing PIL instruments may lead to affirm that these guarantees are otherwise ensured – e.g., the Convention No 108+ will introduce a follow-up mechanism to ensure its correct implementation (see its Article 4). Anyway, these reflections would go beyond the current contribution, and they will be addressed on due course.

SUGGESTED READINGS

Case-law:

CJEU, Judgment of 31 March 1971, *Commission of the European Communities v Council of the European Communities (European Agreement on Road Transport)*, C-22/70, EU:C:1971:32.

CJEU, Judgment of 26 February 2013, *Stefano Melloni v Ministerio Fiscal*, C-399/11, EU:C:2013:107.

CJEU, Judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650.

CJEU, Opinion of 26 July 2017, *Opinion 1/15*, EU:C:2017:592.

Doctrine:

A. ANNONI, A. THIENE, *Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Ferrara, 2019.

A. MANGAS MARTÍN, D. J. LIÑÁN NOGUERAS, *Instituciones y Derecho de la Unión Europea*, Madrid, 2020.

C. KUNER, *Transborder Data Flows and Data Privacy Law*, Oxford, 2013.

D. WRIGHT, P. DE HERT, *Enforcing Privacy. Regulatory, Legal and Technological Approaches*, Law, Governance and Technology Series, Vol. 25, Cham, 2016.

E. KOSTA, F. COUDERT, J. DUMORTIER, *Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive*, in *International Review of Law, Computers & Technology*, Vol. 21, No 3, 2007, pp. 347-362.

F. BOHEM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Cham, 2012.

F. SALERNO, *Diritto internazionale. Principi e norme*, Padova, 2020.

F. TASSINARI, *The evolution of Interoperability under the new pre-entry screening procedure: toward the normalization of biometric identification in the area of freedom, security and justice?*, *Sociedad Digital*, 29.11.2020, last consult on 22 June 2021.

F. TASSINARI, *The externalisation of Europe's data protection law in Morocco: an imperative means for the management of migration flows*, in A. DEL VALLE GÁLVEZ (dir.), *Migration and Human Rights in Europe 's Southern External Borders. Actas de las Jornadas del Centro de Excelencia Jean Monnet de la Universidad de Cádiz en Tánger (2019) y Rabat (2020)*, Madrid, forthcoming publication.

G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series, Vol. 16, Cham, 2014.

H. HIJMANS, *Privacy and Data Protection as Values of the EU That Matter, Also in the Information Society*, Law, Governance and Technology Series, Vol. 31, Cham, 2016.

M. BRKAN, *The essence of Fundamental Rights to Privacy and Data Protection: Finding Way Through the Maze of the CJEU's Constitutional Reasoning*, in *German Law Journal*, No 20, 2019, pp. 864-883.

O. LINSKEY, *The Foundations of EU Data Protection Law*, Oxford, 2015.

P. GARCÍA ANDRADE, *La acción exterior de la Unión Europea en materia migratoria. Un problema de reparto de competencias*, Valencia, 2015.

R. PALLADINO, *Efficacia dei rimpatri e tutela dei diritti fondamentali e della dignità dei migranti: quale equilibrio nelle prospettive di riforma della direttiva rimpatri?*, ADiM Blog, Analisi & Opinioni, 30.12.2020, last consult on 22 June 2021.

S. CARRERA, *Implementation of EU Readmission Agreements. Identity Determination Dilemmas and the Blurring of Rights*, Cham, 2016.

S. SALUZZO, *The EU as a Global Standard Setting Actor: The Case of Data Transfers to Third Countries*, in E. CARPANELLI, N. LAZZERINI (edited by), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Cham, 2019, pp. 115-134.

T. FAJARDO DEL CASTILLO, *La Directiva sobre el retorno de los inmigrantes en situación irregular*, in *Revista de Derecho Comunitario Europeo*, No 33, 2009, pp. 453-499.

Other materials:

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Way forward on aligning the former third pillar acquis with data protection rules, COM(2020) 262 final, Brussels, 24.6.2020.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital

transition - two years of application of the General Data Protection Regulation, COM/2020/264 final, Brussels, 24.6.2020.
EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, 15 December 2020.
EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion on the data protection reform package*, 7 March 2012.
PROPOSAL FOR A COUNCIL DECISION authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), COM/2018/451 final, Brussels, 5.6.2018.

To cite this contribution: F. TASSINARI, *Privacy enhancing readmission: the clause on data protection in the EURAs*, ADiM Blog, Analyses & Opinions, 30 June 2021.