



CROSS-BORDER TRANSFERS OF PERSONAL DATA UNDER THE GDPR: SCOPE AND LIMITATIONS OF THE “BLOCKING STATUTE”

Martina Drventić Barišin, PhD, Assistant Professor

Josip Juraj Strossmayer University of Osijek, Faculty of Law
Stjepana Radića 13, 31 000 Osijek, Croatia
mdrventic@pravos.hr

ABSTRACT

The General Data Protection Regulation (GDPR) establishes a comprehensive framework for personal data protection within the European Union, with particular emphasis on cross-border data transfers. The GDPR addresses cross-border data protection through two complementary regulatory approaches. First, the rules on territorial scope extend the GDPR's application to certain processing activities conducted by controllers or processors established outside the EU, provided these activities relate to the data of individuals located within the Union. These provisions are intended to protect EU data subjects from external threats posed by non-EU actors. Second, the GDPR sets forth a regime for transfers of personal data to third countries or international organisations. The transfer regime is preventive in nature, as it requires that personal data exported outside the EU continue to benefit from safeguards that are essentially equivalent to those provided under EU law. Prior to any transfer, the parties involved must ensure that appropriate legal safeguards are in place.

Among the relevant provisions, Article 48 of the GDPR, often referred to as the “blocking statute,” plays a distinctive role in regulating transfers of personal data in response to requests from authorities of third countries or international organisations. This provision clarifies that judgments or decisions of courts or administrative authorities of third countries requiring a controller or processor to transfer or disclose personal data do not, in themselves, constitute a legal basis for such transfers. In this way, the EU asserts its legal sovereignty in relation to the laws of third countries, establishing as a general rule that recognition and enforcement of such foreign judgments or decisions may occur only through the application of international agreements.

Throughout the paper, the extraterritorial effects of the GDPR are examined and clarified, with particular emphasis placed on the “blocking statute” rule, as interpreted in relevant legal doctrine, guidance, and the CJEU case law.

Keywords: Blocking statute, Cross-border, Data, GDPR, Transfer

1. INTRODUCTION

Modern protection of the right to privacy and personal data faces important challenges due to fast technological development and globalisation. Digital technologies have greatly increased the volume of personal data collected and shared, allowing individuals to enhance their activities using this data.¹ However, this expansion in data processing can conflict with the effective protection of fundamental human rights.²

Data privacy rights now have a clear transnational dimension. Previously, data controllers, data subjects, and processing activities were usually within one jurisdiction. Now, international trade, new technology, and multinational corporations have made cross-border data processing and transfers routine. In this borderless environment, data protection frameworks limited to a single territory are no longer enough.³ Cross-border data transfers have become hallmarks of globalisation and crucial links in the global economy.⁴

To address these challenges, the European Union created a harmonised data protection framework. Its aim is to ensure a consistent level of protection for individuals in all Member States and beyond.⁵ It also considers that EU data protection law has evolved to handle risks from outside its borders. This protection is firmly embedded in the General Data Protection Regulation (hereinafter: GDPR) and has its roots in the earlier Data Protection Directive 95/46/EC (hereinafter: DPD).⁶ The Court of

¹ 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 L 119 (hereinafter: GDPR), Recital 6.; Ausloos, J., *The Right To Erasure In EU Data Protection Law: From Individual Rights To Effective Protection*, Edition: 1, Oxford University Press, Oxford, 2020, pp. 1 - 11.

² Lopes, D., GDPR – Main International Implications, *European Journal of Privacy Law & Technologies*, Special issue, G. Giappichelli Editore, Torino, 2020, p. 11.

³ Azzi, A., *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 9, No. 2, 2018, p. 127.; Juliussen, BA; Kozyri, E.; Johansen, D.; Rui, JP., *The third country problem under the GDPR: enhancing protection of data transfers with technology*, *International Data Privacy Law*, 2023, Vol. 13, No. 3, p. 225.

⁴ Voss, W. G., *Cross-Border Data Flows, the GDPR, and Data Governance*, *Washington International Law Journal*, Vol. 29, No. 3, 2020, p. 487.

⁵ The protection of natural persons in relation to the processing of personal data is recognized as a fundamental right under Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). This objective permeates all areas of EU competence and policy, including those implemented at the national level.

⁶ 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 L 281, (hereinafter: DPD); See: Hustinx, P., *EU Data Protection Law: The Review of*

Justice of the European Union (hereinafter: CJEU) has consistently noted that data protection rights must be safeguarded internationally and are not restricted to the EU's territorial boundaries.⁷

Recent years have seen growing concern regarding threats to the data protection rights of EU individuals arising from third countries. Noteworthy examples include the alleged misuse of EU personal data by companies established outside the EU, the disclosures concerning mass surveillance by foreign intelligence agencies, and legislative measures such as the US CLOUD Act, which may compel the transfer of data stored within the EU.⁸ In response, EU data protection law relies on two principal regulatory mechanisms: rules governing its territorial scope and rules restricting international data transfers. The former determine the circumstances under which EU data protection law applies extraterritorially, while the latter impose conditions on the transfer of personal data to third countries. Given the significant global influence of EU data protection law, these mechanisms have far-reaching implications beyond the EU's borders.

Article 48, known as the “blocking statut”, is part of the EU's data transfer rules and aims to prevent conflicts between EU data protection law and foreign laws requiring access to personal data. The main argument is that while this mechanism seeks to balance EU privacy requirements with increasing global demands for cross-border evidence and data disclosure, its actual effectiveness is uncertain. This uncertainty stems from the rise of direct-access regimes and large-scale surveillance practices that bypass traditional legal channels.

This paper uses a doctrinal legal research methodology. It examines the extraterritorial effects of the GDPR by analysing the relevant regulatory framework, legal scholarship, regulatory guidance, and the CJEU's jurisprudence. The focus is on the rules governing the territorial scope of EU data protection law and international data transfers. Special attention is given to Article 48 GDPR. By analysing the above-mentioned sources, the paper aims to clarify the role of Article 48 within the GDPR's extraterritorial application. It also provides a preliminary assessment of Article 48's effectiveness in addressing conflicts between EU data protection law and third-country access requests.

Directive 95/46/EC and the General Data Protection Regulation, in: Cremona, M. (ed.), *New Technologies and EU Law*, Oxford University Press, Oxford, 2017, pp. 148 - 151.

⁷ E.g. Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* [2020] ECLI:EU:C:2020:559; Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2025, p. 42.

⁸ Kuner, C., *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*, University of Cambridge Faculty of Law Research Paper No. 20/2021, 2021, p. 3.

2. GDPR'S GLOBAL IMPACT

The EU aims to be a global regulator based on several interrelated factors, among them digitalisation, which plays a central role. The rise of digital technologies has made interactions more immaterial and separated from physical territory. Traditional ideas of territoriality are now less effective in addressing regulatory challenges in the digital environment.⁹ The scope of EU's instruments must include activities outside the Member States that could affect or undermine the Union's interests. EU law in this area covers not only individuals and entities in the Union, but also those in third countries whose activities target Member States *via* the internet or digital technologies.¹⁰

EU rules on privacy and data protection have come to shape the global regulatory landscape in a profound way, both in practice and through formal legal influence, reflecting what is commonly described as the "Brussels Effect". In this sense, data protection law stands out as a key vehicle through which European regulatory standards extend beyond the Union's borders and contribute to broader processes of global Europeanization.¹¹ Given the global nature of data processing and the critical role of cross-border data flows, not only within the EU but across global markets, the EU has recognised the need to promote international standards for personal data protection. The EU seeks to help shape global data privacy standards. It also underlines the risk that alternative global standards may be less desirable, for instance by imposing data localisation requirements or by using data protection as a tool for censorship and state surveillance.¹² This intention was clear when proposing the GDPR, as the Commission indicated that the 'individuals'

⁹ Chia, CW., *Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction*, Singapore Academy of Law Journal, Vol. 30, No. 2, 2018, pp. 833 – 870.; Benvenuti, E., *Private International Law as a Means to Project EU Digital Values Abroad*, EU and comparative law issues and challenges series, Special Issue - Law in the Age of Modern Technologies, Vol. 7, 2023, p. 229.

¹⁰ Benvenuti, *op. cit.*, note 9, 229.; E.g. provisions on territorial scope in: GDPR, Art. 3, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, 2024/1689, Art (2)(1); Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, Art 2(1).

¹¹ Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2019, p. 132.; see also: Gstrein, OJ; Zwitter, AJ, *Extraterritorial application of the GDPR: promoting European values or power?*, Internet Policy Review, Vol. 10, No. 3, 2021, p. 1-30.; Hornkohl, L., *The Extraterritorial Application of Statutes and Regulations in EU Law*, Max Planck Institute Luxembourg for Procedural Law Research Paper Series, No. 2022 (1), pp. 3-4.

¹² Bradford, *op. cit.*, note 11, p. 137.

rights must continue to be ensured when personal data is transferred from the EU to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third country service providers.¹³ GDPR seeks to achieve those ambitious goals by a combination of rules on territorial scope and international data transfers. The following sections of this paper will explore these mechanisms in greater detail.

The CJEU's activism further shapes this policy. The first case on cross-border data transfers was *Lindqvist*, which clarified that uploading personal data to a website hosted within the EU does not count as a transfer to a third country under the DPD.¹⁴ The landmark *Google Spain* judgment of the CJEU established that EU data protection law can apply to a search engine service operated by a company headquartered outside the EU. This judgment illustrates a broader effort to adapt traditional legal concepts to the inherently non-territorial nature of cyberspace.¹⁵ In *Google LLC*, the CJEU further affirmed that the operation of a search engine in a third country, when inextricably linked to an establishment of the company in the EU, could not avoid the protections of the DPD and the GDPR. The Court held that, in its current form, the GDPR does not require the right to be forgotten to extend to all national versions of search engines. However, it noted that the EU legislator could choose to broaden the Regulation's scope in the future. The Court also clarified that national courts and supervisory authorities are not precluded from ordering such an extension.¹⁶

This expansive approach was reinforced in the *Schrems* litigation, highlighting how individual activism can trigger global regulatory change.¹⁷ Max Schrems,

¹³ Kuner, *op. cit.*, note 8, p. 5.; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century, COM(2012) 9/3, 25 January 2012, p. 10.

¹⁴ Case C-101/01, *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596, para 52-71. This position is confirmed in the context of chapter V of the GDPR.; see: Coetzee, J., *Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part II: The Data Transfer Provision*, Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, Vol. 27, 2024, p. 9.

¹⁵ C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317; see: Van A., Brendan; Koekkoek, M., *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'*, International Data Privacy Law, Vol. 5, No. 2, 2015, pp. 105 – 120.

¹⁶ C-507/17 *Google LLC v CNIL* [2019] ECLI:EU:C:2019:772., para 51.; Coetzee, *op. cit.*, bilj. 14, p. 10.; Quinn, J., *Google v CNIL: Circumscribing the Extraterritorial Effect of EU Data Protection Law*, in: Fabbrini, F.; Celeste, E.; Quinn, J., *Data Protection Beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, 2021, pp. 47. – 63; Samonte, M., *Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law*, European Papers, Vol. 4, No. 3, 2019, pp. 839-851.

¹⁷ Bradford, *op. cit.*, note 11, p. 139.

an Austrian lawyer and data protection activist, challenged Facebook's data practices after discovering how much personal data the company collected on him. His complaints, lodged first with the Irish Data Protection Commission, led to a CJEU reference. In its decision, the Court invalidated the EU–US Safe Harbour framework, emphasising that data transferred outside the EU must be protected at a level essentially equivalent to that within the EU.¹⁸ In *Schrems II*, the Court upheld standard contractual clauses (SCCs) but struck down the EU–US Privacy Shield, Safe Harbour's successor.¹⁹ The Court confirmed that “essential equivalence” under Article 45 GDPR also applies to SCCs under Article 46 and must be assessed under EU law, particularly the Charter, not Member State law.²⁰ With *Schrems II*, the CJEU strongly reaffirmed the need to ensure a high level of protection for personal data transferred from the EU to third countries, addressing government access not only in the United States but globally. Subsequent decision went beyond *Schrems I* by completing the conceptual framework for data transfers, aiming to prevent circumvention of GDPR standards.²¹ The decisions in these cases have significantly influenced the interpretation and application of the GDPR's provisions and have clearly highlighted the need for further discussion on its extraterritorial application.²²

3. EXTRATERRITORIAL APPLICATION OF THE GDPR REGULATION

The GDPR seeks to protect personal data from external threats primarily through its rules on territorial scope, as set out in Article 3, and through the restrictions on data transfers contained in Chapter V.²³

¹⁸ C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.; see: Catanzariti, M., *Off-line Digital Jurisdiction*, EUI Working paper, RSCAS 2019/03, Robert Schuman Centre for Advanced Studies p. 12.

¹⁹ Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559.

²⁰ See: Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* C-311/18, ECLI:EU:C:2019:1145., paras 111. – 120.

²¹ Christakis, T., *The “Zero Risk” Fallacy: International Data Transfers, Foreign Governments’ Access to Data and the Need for a Risk-Based Approach*, CIPL/CBDF Paper Series, 2024., p 11.; see also: CJEU's *Opinion 1/15* [2017] ECLI:EU:C:2017:592.

²² Tzanou, M., *Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights*, in: Fabbrini, F.; Celeste, E.; Quinn, J., *Data Protection Beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, 2021, p. 116.

²³ Significantly, Article 27 prescribes the obligation to designate the Representatives of controllers or processors not established in the Union. That requires a special substantive obligation for undertakings in international situations. It underscores the need for a “guarantor” within the European Union, a repre-

Territorial scope rules are *inward-looking* in that they are designed to protect individuals in the EU from actions taken by actors outside its borders, and they operate reactively, applying when non-EU parties engage in certain activities involving the data of individuals in the EU. By contrast, data transfer rules are *outward-looking*, requiring that personal data transferred to third countries be afforded a level of protection grounded in EU law. They are also proactive in nature, addressing risks before the transfer takes place by requiring the parties involved to ensure an adequate level of protection prior to initiating the transfer.²⁴

As the territorial scope is not the main focus of this paper, it will be addressed only briefly, with emphasis on its effects. Article 3 GDPR states that the Regulation applies to data processing in the context of activities of an establishment in the EU, regardless of where the processing occurs. It also applies to non-EU controllers or processors if their processing involves offering goods or services to individuals in the EU or monitoring their behaviour within the Union, as long as the data subjects are located in the EU at the relevant time.²⁵ Unlike the DPD, which in Article 4 specified the applicable national law to distinguish between Member States, Article 3 of the GDPR defines the territorial scope of its uniform rules to set them apart from third country laws.²⁶ The name of Article 3, Territorial scope, should not be taken literally. Rather, this provision identifies the types of connections to EU territory that trigger the GDPR's application.

The rules set out in Article 3 are mandatory and cannot be derogated from, meaning that any attempt to alter them, such as through contractual clauses or privacy

sentative who should not only act on behalf of the controller or the processor but also be addressed by supervisory authorities. Article 27 provides data subjects and supervisory authorities with an additional (or alternative) point of contact (i.e., the representative) for all issues regarding the processing of personal data, while at the same time maintaining their right to initiate legal actions directly against the controllers or processors.; See: Millard, C.; Kamarinou, D., *Article 27. Representatives of controllers or processors not established in the Union*, in Kuner, C.; Bygrave, Lee A.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, pp. 589 - 599.

²⁴ Kuner, C. B., *Protecting EU Data Outside EU Borders under the GDPR*, Common Market Law Review, Vol. 60, No. 1, p. 79.

²⁵ For scientific analyses see: Svantesson, D. J. B., *Article 3. Territorial scope*, in: Kuner, C.; Bygrave, Lee A.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, pp. 74 -100; Kunda, I., *Prekogranična provedba prava na zaštitu osobnih podataka u Europskoj uniji*, in: Barbić, J.; Župan, M. (eds.), *Identitet u prekograničnim privatnopravnim odnosima*, Hrvatska akademija znanosti i umjetnosti, Zagreb, 2021, pp. 141.-169.; also see the relevant CJEU practice in: C-131/12 *Google Spain* [2014] EU:C:2014:317; C-230/14 *Weltimmo* [2015] EU:C:2015:639, C-191/15 *Verein für Konsumenteninformation* [2016] EU:C:2016:61, C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] EU:C:2018:388; C-507/17 *Google Inc. vs CNIL* [2019] EU:C:2019:772.

²⁶ Kunda, *op. cit.*, note 25, p. 147.

policies specifying alternative jurisdiction or choice-of-law rules, will be considered invalid by courts or data protection authorities.²⁷ For this reason, it may be argued that the GDPR could potentially qualify as overriding mandatory provisions within the meaning of Article 9 of the Rome I Regulation.²⁸ Current doctrine remains divided on whether EU data protection law is mandatory in nature. Some theorists argue that Article 3 can be interpreted as overriding mandatory provisions.²⁹ Deriving from the *Ingmar* case, it follows that where EU mandatory rules aim to protect a weaker party, and there is a close connection to the EU, there is a presumption that such rules qualify as overriding mandatory provisions.³⁰ This is further supported by the fact that there are explicitly prescribed conditions under which the processing of personal data is considered lawful, as well as by the impossibility of derogating from data subjects' rights and the obligations of controllers by agreement. The GDPR was adopted in the public interest, which is also reflected in the way supervision of its application is organised.³¹ On the other hand, it is argued that Article 3 cannot be characterised as a rule of direct application, as it merely establishes that the substantive provisions of the GDPR apply in an international context. This can be considered justified, given that rules of direct application are of a substantive nature.³² Interpreted narrowly, Article 3 should be understood as a provision defining the territorial scope of directly applicable rules.³³

²⁷ Svantesson, *op. cit.*, note 25, p. 82.

²⁸ Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177, Article 9(1): "Overriding mandatory provisions are provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract under this Regulation."

²⁹ Thon, M., *Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO*, *Rabels Zeitschrift für ausländisches und internationales Privatrecht / The Rabel Journal of Comparative and International Private Law*, Bd. 84, H. 1, 2020, p. 41.

³⁰ C-381/98 *Ingmar GB* [2000] ECLI:EU:C:2000:605.

³¹ Kohler, C., *Conflicts of Law Issues in the 2016 Data Protection Regulation of the European Union*, *Rivista di diritto internazionale privato e processuale*, Vol. 52, No. 3, 2016, p. 661; Brkan, M., *Data Protection and Conflicts of Laws, A Challenging Relationship*, *European Data Protection Law Review*, Vol. 2, No. 3, 2016, p. 333.

³² Melcher, M., *Substantive EU Regulations as Overriding Mandatory Rules*, *ELTE Law Journal*, No. 1, 2020, p. 24.; Wilderspin, M., *Overriding mandatory provisions*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), *Encyclopedia of Private International Law*, Volume 2, Edward Elgar, Cheltenham, 2017, pp. 1331 - 1336.

³³ EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, Version 2.1, 12 November 2019, p. 5.; Vrbljanac, D., *Zaštita osobnih podataka i međunarodno privatno pravo*, in: Barbić, J. (ed.), *Međunarodno privatno pravo i globalni trendovi*, Hrvatska akademija znanosti i umjetnosti, Zagreb, p. 145.

The GDPR's rules on international data transfers,³⁴ set out in Chapter V, build upon the framework established under the DPD, retaining its three main transfer mechanisms with only minor modifications. Their overarching purpose remains the prevention of circumvention of EU data protection law. This objective is reflected in Article 44, which requires that transfers be carried out in a manner that does not undermine the level of protection guaranteed by the GDPR, including in the case of subsequent (onward) transfers to other third countries or international organisations. As emphasised by the EDPB in light of the Schrems II judgment, the protection afforded to personal data within the European Economic Area must effectively "travel with the data" wherever it is transferred. Similar to the rules on territorial scope, the data transfer regime extends the reach of the GDPR beyond the EU, thereby imposing obligations on entities located in third countries.³⁵

To ensure an essentially equivalent level of protection, the GDPR establishes a three-tiered system of legal bases for transfers: adequacy decisions, appropriate safeguards, and derogations. Adequacy decisions, adopted by the European Commission, confirm that a third country or international organisation ensures an adequate level of protection; in their absence, transfers may rely on appropriate safeguards, such as standard contractual clauses or binding corporate rules; only where neither is available may derogations be invoked as exceptions. This hierarchical structure underscores the priority of systemic and stable transfer mechanisms over exceptional ones.³⁶ The rationale underlying this regime reflects a balance between enabling the free flow of personal data and ensuring a consistently high level of protection.³⁷ While international data flows are recognised as essential, they must not lead to a lowering of protection standards. In this sense, the prohibition against undermining the level of protection can be understood as a prohibition of circumvention, preventing personal data from being transferred to jurisdictions where EU safeguards could be effectively bypassed.

³⁴ The GDPR does not define what constitutes an international data transfer (just as the DPD did not). This concept is central, as it determines when Article 44 (and the other provisions of Chapter V) applies. By contrast, Article 4(23) defines 'cross-border processing', which might seem similar but actually refers to situations involving a controller or processor with establishments in more than one Member State, or where processing substantially affects data subjects in more than one Member State, specifically to help determine the lead supervisory authority under Article 56.

³⁵ Kuner, *op. cit.*, note 8, p. 15; EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, (10 November 2020) (version for public consultation), p. 2.

³⁶ Kuner, C., *Article 44. General principle for transfers*, in: Kuner, C.; Bygrave, Lee A.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, p. 765.

³⁷ GDPR, Recital 101.

4. “BLOCKING STATUTE”

The central focus of this paper is the so-called “blocking statute” mechanism,³⁸ as embodied in Article 48 GDPR. Entitled “Transfers or disclosures not authorised by Union law,” this provision forms part of Chapter V, which governs cross-border data transfers. In contrast to the other provisions of the Chapter V of the GDPR, Article 48 does not constitute a ground for transfer. By contrast, this rule is more appropriately characterised as a transfer safeguard. Consequently, when faced with a request from a third-country authority covered by Article 48, the controller or processor must rely on a separate transfer mechanism provided elsewhere in Chapter V before disclosing the data.³⁹

The rationale behind the Article 48 is explained by the Recital 115, emphasizing that laws or decisions of third countries should not undermine the level of data protection guaranteed within the EU. Building on this objective, Article 48 provides that judgments or administrative decisions of third-country authorities requiring the disclosure of personal data are not, by themselves, a valid legal basis for a transfer. This rule reinforces the general principle established in Article 44, according to which any transfer of personal data to a third country must comply with the safeguards of Chapter V GDPR and ensure that the level of protection guaranteed by the Regulation is not compromised.

The rule on “blocking statute” is designed to limit the extraterritorial jurisdiction of courts, tribunals, or authorities in third countries. It does so by stating that any third-country judgment or administrative decision requiring a controller or processor to transfer or disclose personal data can only be recognised or enforced if it is based on an international agreement, such as a mutual legal assistance treaty, in force between the third country and the Union or a Member State.

This chapter will further examine the background and nature, as well as the conditions and consequences of its application, in order to reach a comprehensive conclusion on its scope and limitations, taking into account its regulatory framework and interpretations derived from legal theory and relevant guidelines.

4.1. Nature and Background of the GDPR’s “Blocking Statute” Rule

Article 48, despite its title, does not address “transfers or disclosures not authorised by Union law” generally. Instead, it focuses on the recognition and enforcement of

³⁸ See: Hemler, A., *Deconstructing blocking statutes: why extraterritorial legislation cannot violate the sovereignty of other states*, *Journal of Private International Law*, Vol. 21, No. 1, 2025, pp. 115-134; Audit, M.; Basedow, J., *Blocking Statutes*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), *Encyclopedia of Private International Law*, Volume 2, Edward Elgar, Cheltenham, 2017, pp. 209 – 214.

³⁹ EDPB, *Guidelines 02/2024 on Article 48 GDPR*, Version 2.1, Adopted on 4 June 2025., p. 11.

judgments and decisions issued by courts, tribunals, and administrative authorities from third countries. It is best understood as a “blocking statute” tailored to data protection.⁴⁰ “Blocking statutes” are a form of countermeasures in public international law. When one state views another’s actions as unlawful, offensive, or against its interests, it may respond with such measures in various forms.⁴¹ The primary purpose of “blocking statutes” is political. They aim to increase pressure on the foreign government whose policies are opposed, using individuals and corporate entities as instruments.⁴² “Blocking statutes” have been used rarely, and their application often ceases once the legal conflict is resolved, typically through an international agreement.⁴³

The key issue is whether the same can be expected in relation to Article 48, considering that government demands for access to data stored abroad are a global phenomenon, not confined to the United States. Moreover, the challenges associated with Article 48 are likely to be even more significant when such requests originate from third countries not having the same standards of human rights and the rule of law.⁴⁴

Article 48 addresses situations in which conflicts arise between the laws and policies of the EU and those of third countries. Such situations, involving the transfer or access to data from the EU without a lawful basis under EU law, have not been uncommon in the past. An early impetus for such legislation dates back to the period of the Second World War and the Nazi misuse of personal data of Jews and other persecuted minority groups.⁴⁵ Significant drivers also arose from situations involving the United States. There are examples of US requirements concerning discovery, the process in civil litigation that enables parties to obtain information and evidence from opposing parties. U.S. courts have interpreted these obligations as extending to discovery conducted outside the United States, even after the US became a party to the Hague Evidence Convention.⁴⁶ Speaking of violations of the right to privacy abroad, it is also essential to mention access by governmental au-

⁴⁰ See: Christakis, T., *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR*, 2019, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3397047, Accessed 8 April 2026.

⁴¹ Basedow, *op. cit.* note 38, p. 209.

⁴² *Ibid.*, p. 214.

⁴³ *Ibid.*

⁴⁴ Kuner, C., Article 48. *Transfers or disclosures not authorised by Union law*, in: Kuner, C.; Bygrave, Lee A.; Docksey, C.; Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, p. 828.

⁴⁵ Bradford, *op. cit.*, note 11, p. 136.

⁴⁶ Kuner, *op. cit.*, note 44, p. 826.; see: WP29 2009: Article 29 Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, (WP 158, 11 February 2009).

thorities to personal data for law enforcement, anti-terrorism, or national security purposes. The most well-known example is the so-called “Snowden revelations,” which exposed extensive electronic surveillance by U.S. intelligence agencies and gained global attention in 2013,⁴⁷ and the recent example of the US Clarifying Lawful Overseas Use of Data (CLOUD) Act 9.⁴⁸

4.2. Conditions to Data Transfer. Two step-approach.

The EDPB introduced the so-called two-step test for data transfers in its Guidance on Article 48. This means that compliance with foreign judgments and decisions under Article 48 is only permissible if there is a legal basis under Article 6 and the provisions of Chapter V of the GDPR. This is clarified by specifying that when data processed in the EU are transferred or disclosed in response to a direct request from an authority in a third country, such disclosure falls under the GDPR and qualifies as a transfer within the meaning of Chapter V. Consequently, as with any GDPR-regulated transfer, there must be a legal basis for processing under Article 6, as well as a valid transfer mechanism under Chapter V. In addition to complying with the GDPR, controllers or processors may also be required to meet further obligations arising from other legal instruments, such as national procedural laws or international agreements governing cooperation with the requesting third-country authority.⁴⁹

Article 48 addresses situations in which a court, tribunal, or administrative authority of a third country requires a controller or processor in the EU to transfer or disclose personal data. Such requests may only be recognised or enforced if they are based on an applicable international agreement that may create a legal obligation for the controller. In such cases, Article 6(1)(c), in conjunction with Article 6(3), may provide the appropriate legal basis for the processing. An “applicable international agreement” refers to one allowing direct requests from third-country public authorities to private entities in the EU. Where no such agreement exists, but cooperation is governed by instruments such as mutual legal assistance trea-

⁴⁷ Cate, F. H.; Dempsey, J. X.; and Rubenstein, I. S., *Systematic Government Access to Private-Sector Data*, International Data Privacy Law, Vol. 2, No. 4, 2012, p. 195.; Coyne, H., *The Untold Story of Edward Snowden's Impact on the GDPR*, The Cyber Defense Review, Vol. 4, No. 2, 2019, pp. 65 – 80.

⁴⁸ Greenwald, G., *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, MacMillan, New York, 2014; Milanovic, M., *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, Harvard International Law Journal, Vol. 56, No. 1, 2015, p. 81.; EDPS Response Cloud Act: European Data Protection Board and European Data Protection Supervisor, ‘EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex)’ (10 July 2019).

⁴⁹ EDPB, *op. cit.* note 39., p. 8.

ties (MLATs), the request should generally be channelled through the competent national authority.⁵⁰

Article 48 does not, in itself, constitute a legal ground for transfer. Instead, it clarifies that foreign decisions cannot have an effect in the EU without an international agreement.⁵¹ Consequently, controllers must identify a valid transfer mechanism under Chapter V before responding to such requests. Article 48 must be read together with Article 44. Article 44 establishes that transfers must comply with all GDPR requirements and ensure the level of protection is not undermined (the so-called two-step test). Chapter V provides a hierarchy of transfer mechanisms: adequacy decisions under Article 45, appropriate safeguards under Article 46, and, only in limited cases, derogations under Article 49. International agreements may qualify as appropriate safeguards⁵² if they are legally binding and enforceable instruments between public authorities and include sufficient protections. According to the EDPB, such agreements must ensure a level of protection essentially equivalent to that in the EU. This includes enforceable data subject rights, limitations on onward transfers, and effective supervision and redress mechanisms.⁵³

Where no adequate international agreement exists, or where it lacks sufficient safeguards, controllers must rely on another transfer ground. Derogations under Article 49 remain a last resort and must be interpreted restrictively, typically applying only in exceptional and non-repetitive situations.⁵⁴ The EDPB has further emphasised that reliance on these derogations to justify transfers in response to foreign requests will generally be difficult in practice.⁵⁵

4.3. The Scope and Limitation of the “Blocking Statute”

Once the conditions for the application of Article 48 are fulfilled, a judgment or decision may be “recognised or enforced” only if, in any manner, it is based on an international agreement. According to the EDPB Guidelines, the application of Article 48 should lead controllers and processors to refuse the transfer of personal

⁵⁰ *Ibid.*, p. 7 – 9.; Kuner, *op. cit.*, note 44, 831. See also: Shurson, J., *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, International Journal of Law and Information Technology, Vol. 28, 2020, p. 173.

⁵¹ EDPB, *op. cit.*, note 39, p. 9.

⁵² GDPR, Art 46(2): “a legally binding and enforceable instrument between public authorities or bodies”

⁵³ EDPB, *op. cit.*, note 39, p. 12. See also: See in this regard part 2 of the EDPB Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b).

⁵⁴ Kuner, *op. cit.*, note 44, p. 831.

⁵⁵ EDPB, *op. cit.*, note 39, p. 12.

data and instead refer foreign authorities to the relevant international agreement.⁵⁶ The provision on the “blocking statute” manifests its effect through the conditions for the recognition and enforcement of a foreign judicial or administrative decision. Therefore, it appears to apply only when such recognition or enforcement is sought. However, the EDPB interprets it somewhat more broadly, namely as a prohibition on data controllers and data processors from disclosing or transferring personal data in response to requests from foreign governments.⁵⁷

Recognition and enforcement of foreign judicial decisions is a field of private international law that deals with extending the legal effects of a foreign court decision to the territory of the state of recognition, allowing the applicant to enforce it using domestic enforcement mechanisms.⁵⁸ The term “recognition and enforcement,” however, is used in a more formal sense in Article 48; therefore, a data controller or data processor cannot be said to be in a position to “recognise and enforce” a foreign judicial decision merely by transferring personal data to a foreign party that has requested it.⁵⁹

The EDPB adopts a broader reading, relying on the article’s title, which suggests a general prohibition on unauthorised data transfers to third countries. However, the actual wording of Article 48 appears much narrower, focusing specifically on the recognition and enforcement of foreign judicial or administrative decisions. Although Recital 115 emphasises that transfers must comply with the GDPR rules on third-country transfers, it largely reiterates Article 44 rather than expanding on Article 48. As a result, the mismatch between the article’s broad title and its more limited text creates uncertainty and potential confusion about its true scope.⁶⁰

The formal recognition and enforcement of decisions of third countries is governed by numerous international agreements to which the EU and/or its Member

⁵⁶ EDPB, *op. cit.*, note 39, p. 9.

⁵⁷ EDPB, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, Available at: [https://www.edps.europa.eu/sites/default/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf], Accessed 5 May 2026.

⁵⁸ Gascón Inchausti, F., *Chapter 12, Recognition and Enforcement: Fundamental Issues*, in: Kramer, X.; Voet, S.; Dori, A., *European Civil Procedure*, De Gruyter, Berlin, 2026, p. 239; Domej, T., *Recognition and enforcement of judgments (civil law)*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), *Encyclopedia of Private International Law*, Volume 2, Edward Elgar, Cheltenham, 2017., pp. 1472 - 1479.

⁵⁹ Kuner, *op. cit.*, note 44, p. 833.

⁶⁰ *Ibid.*, p. 834.

States are parties. This is the case, for example, with formal requests (*Letters Rogatory*) sent by judicial authorities of a state party to the Hague Evidence Convention to the judicial authority of another contracting state, which are then executed in accordance with the methods and procedures provided for under national law.⁶¹

However, widespread electronic surveillance, which was one of the reasons for introducing such provisions, does not fall within the scope of Article 48, since it involves authorities of third countries that do not, in practice, seek prior recognition and enforcement of their decisions from data controllers or data processors in the EU. In this sense, the intention of EU legislation to fully protect against unauthorised access to personal data has not been entirely realised.⁶²

Among other things, the provision requires an international agreement as a condition for a third country's decision to be recognised and enforced. This should mean that such a decision must either be provided for by, or issued in accordance with, an international agreement. The most obvious example is a decision of a national court issued pursuant to the Hague Evidence Convention, which provides for the taking of evidence based on requests from national courts directly addressed to the competent authorities of the contracting states.⁶³ The question that arises is which international agreements may fall within the scope of Article 48. With regard to agreements concluded between the EU and a third country, it is clear that they must fall within the scope of EU law and meet the definition of an international agreement within the meaning of Title V of the Treaty on the Functioning of the European Union.⁶⁴ International agreements in force between a third country and a Member State, such as the Hague Evidence Convention (to which some but not all EU Member States are parties), and MLATs, are expressly covered by Article 48.

The question also arises whether Article 48 covers international agreements that fall within EU law but outside the GDPR's scope. The legislator is not specific, stating only that data transfers to third countries must follow international agreements. This suggests Article 48 should not be interpreted too restrictively.

⁶¹ See: Marshall, B.; de Araujo, N., *Taking of Evidence*, in: Beaumont, P.; Holliday, J. (eds.), *A Guide to Global Private International Law*, Hart Publishing, 2022, pp. 175 – 191.

⁶² Kuner, *op. cit.*, note 44, p. 834.; Schantz, P., *Article 48. GDPR Transfers or disclosures not authorised by Union law*, in: Spiecker Döhmman, I.; Papakonstantinou, V.; Hornung, G.; De Hert, P. (eds.), *General Data Protection Regulation: Article-by-Article Commentary*, Nomos, 2023.

⁶³ HCCH, Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, Art. 1. See: Hartley, T. C., *International Commercial Litigation. Text, Cases and Materials on Private International Law*, Cambridge, 2015, p. 529.

⁶⁴ See: C-327/91, *French Republic v Commission* [1994] ECLI:EU:C:1994:305, para. 27.

Building on this, Article 48 should also apply to agreements that do not fall within the scope of the GDPR, as long as they are within the scope of EU law and provide “an appropriate level of protection for the fundamental rights of data subjects.” This point is particularly relevant given that Article 48 itself does not specify the data protection standards that international agreements must meet. Furthermore, while data protection is not mentioned in most international agreements, it has increasingly begun to appear as a standard in agreements on mutual legal assistance.⁶⁵

5. CONCLUSION

The analysis of cross-border data transfers under the GDPR clearly shows that the EU is keen to establish a high and globally relevant level of data protection through a combination of rules on territorial scope and restrictions on cross-border transfers.

In this context, Article 48, the so-called “blocking statute”, plays a significant normative role in maintaining the EU’s regulatory sovereignty. It does so by clearly emphasizing that requests or decisions from authorities of third countries cannot, by themselves, serve as a legal basis for the transfer of data from the EU without a relevant international legal framework.

Despite this important role, the actual scope and effectiveness of Article 48 remain quite limited. Its practical application depends on the existence of international agreements that ensure an adequate level of protection. Where such agreements do not exist, data controllers must rely on other mechanisms from Chapter V of the GDPR, often in restrictive and legally uncertain circumstances.

Additionally, contemporary methods of accessing data, such as direct requests by foreign authorities or large-scale mass surveillance, bypass formal mechanisms for the recognition and enforcement of foreign decisions, thereby falling outside the scope of Article 48.

The inconsistency between the title of Article 48, which suggests a broad prohibition of unauthorised data transfers, and its narrower normative content creates legal uncertainty regarding its actual scope. Such a discrepancy leaves room for differing interpretations, particularly as to whether the provision also covers situations beyond the formal recognition and enforcement of foreign decisions. Additionally, the insufficiently precise definition of the scope of international agreements that may serve as a legal basis for data transfers points to the need for a

⁶⁵ Kuner, *op. cit.*, note 44, p. 835.

broader and more flexible approach, but at the same time for clearer normative regulation.

Although the “blocking statute” is an important tool for protecting personal data and preventing circumvention of the GDPR, it still cannot fully address challenges posed by the modern digital society. Therefore, further international cooperation and clearer rules are needed to balance the protection of EU citizens’ fundamental rights with third-country requests for data transfers. Going forward, the GDPR should more clearly regulate cross-border access requests by third-country authorities and clarify the role of international agreements in data transfers. A clearer Article 48 would help prevent inconsistent interpretations and ensure the provision fits modern digital data flows.

REFERENCES

BOOKS AND ARTICLES

1. Audit, M.; Basedow, J., *Blocking Statutes*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), *Encyclopedia of Private International Law*, Volume 2, Edward Elgar, Cheltenham, 2017., pp. 209 – 214
2. Ausloos, J., *The Right To Erasure In EU Data Protection Law: From Individual Rights To Effective Protection*, Edition: 1, Oxford University Press, Oxford, 2020
3. Azzi, A., *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 9, No. 2, 2018, pp. 126 – 137
4. Benvenuti, E., *Private International Law as a Means to Project EU Digital Values Abroad*, *EU and comparative law issues and challenges series, Special Issue - Law in the Age of Modern Technologies*, Vol. 7, 2023, pp. 227 – 226
5. Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2019
6. Brkan, M., *Data Protection and Conflicts of Laws, A Challenging Relationship*, *European Data Protection Law Review*, Vol. 2, No. 3, 2016, pp. 324 – 341
7. Catanzariti, M., *Off-line Digital Jurisdiction*, EUI Working paper, RSCAS 2019/03, Robert Schuman Centre for Advanced Studies
8. Cate, F. H.; Dempsey, J. X., and Rubenstein, I. S., *Systematic Government Access to Private-Sector Data*, *International Data Privacy Law*, Vol. 2, No. 4, 2012, pp. 195 – 199
9. Chia, CW., *Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction*, *Singapore Academy of Law Journal*, Vol. 30, No. 2, 2018, pp. 833–870
10. Christakis, T., *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR*, 2019, Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3397047], Accessed 8 April 2026

11. Christakis, T., *The “Zero Risk” Fallacy: International Data Transfers, Foreign Governments’ Access to Data and the Need for a Risk-Based Approach*, CIPL/CBDF Paper Series, 2024
12. Coetzee, J., *Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part II: The Data Transfer Provision*, Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, Vol. 27, 2024
13. Coyne, H., *The Untold Story of Edward Snowden’s Impact on the GDPR*, The Cyber Defense Review, Vol. 4, No. 2, 2019, pp. 65 – 80
14. Domej, T., *Recognition and enforcement of judgments (civil law)*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), *Encyclopedia of Private International Law*, Volume 2, Edward Elgar, Cheltenham, 2017., pp. 1472 – 1479
15. Gascón Inchausti, F., *Chapter 12, Recognition and Enforcement: Fundamental Issues*, in: Kramer, X.; Voet, S.; Dori, A., *European Civil Procedure*, De Gruyter, Berlin, 2026, pp. 239 – 261
16. Greenwald, G., *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, MacMillan, New York, 2014
17. Gstrein, OJ; Zwitter, AJ, *Extraterritorial application of the GDPR: promoting European values or power?*, Internet Policy Review, Vol. 10, No. 3, 2021
18. Hartley, T. C., *International Commercial Litigation. Text, Cases and Materials on Private International Law*, Cambridge, 2015
19. Hemler, A., *Deconstructing blocking statutes: why extraterritorial legislation cannot violate the sovereignty of other states*, *Journal of Private International Law*, Vol. 21, No. 1, 2025, pp. 115-134
20. Hornkohl, L., *The Extraterritorial Application of Statutes and Regulations in EU Law*, Max Planck Institute Luxembourg for Procedural Law Research Paper Series, No. 2022 (1)
21. Hustinx, P., *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation*, in: Cremona, M. (ed.), *New Technologies and EU Law*, Oxford University Press, Oxford, 2017, pp. 148 – 151
22. Juliussen, BA; Kozyri, E.; Johansen, D.; Rui, JP., *The third country problem under the GDPR: enhancing protection of data transfers with technology*, *International Data Privacy Law*, 2023, Vol. 13, No. 3, pp. 225 – 243
23. Kohler, C., *Conflicts of Law Issues in the 2016 Data Protection Regulation of the European Union*, *Rivista di diritto internazionale privato e processuale*, Vol. 52, No. 3, 2016, pp. 653 – 675
24. Kunda, I., *Prekogranična provedba prava na zaštitu osobnih podataka u Europskoj uniji*, in: Barbić, J.; Župan, M. (eds.), *Identitet u prekograničnim privatnopravnim odnosima*, Hrvatska akademija znanosti i umjetnosti, Zagreb, 2021, pp. 141 – 169
25. Kuner, C., *Article 44. General principle for transfers*, in: Kuner, C.; Bygrave, Lee A.; Docksey, C., Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, pp. 755 – 770
26. Kuner, C., *Article 48. Transfers or disclosures not authorised by Union law*, in: Kuner, C.; Bygrave, Lee A.; Docksey, C., Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, pp. 825 – 840

27. Kuner, C., *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*, University of Cambridge Faculty of Law Research Paper No. 20/2021, 2021
28. Lopes, D., GDPR – Main International Implications, *European Journal of Privacy Law & Technologies*, Special issue, G. Giappichelli Editore, Torino, 2020
29. Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2025
30. Marshall, B.; de Araujo, N., *Taking of Evidence*, in: Beaumont, P.; Holliday, J. (eds.), *A Guide to Global Private International Law*, Hart Publishing, 2022, p. 175 – 191
31. Melcher, M., *Substantive EU Regulations as Overriding Mandatory Rules*, *ELTE Law Journal*, No. 1, 2020, pp. 37 – 50
32. Milanovic, M., *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, *Harvard International Law Journal*, Vol. 56, No. 1, 2015, pp. 81 – 146
33. Quinn, J., *Google v CNIL: Circumscribing the Extraterritorial Effect of EU Data Protection Law*, in: Fabbrini, F.; Celeste, E.; Quinn, J., *Data Protection Beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, 2021, pp. 47 – 63
34. Samonte, M., *Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law*, *European Papers*, Vol. 4, No. 3, 2019, pp. 839-851
35. Schantz, P., *Article 48. GDPR Transfers or disclosures not authorised by Union law*, in: Spiecker Döhmman, I.; Papakonstantinou, V.; Hornung, G.; De Hert, P. (eds.), *General Data Protection Regulation: Article-by-Article Commentary*, Nomos, 2023
36. Shurson, J., *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, *International Journal of Law and Information Technology*, Vol. 28, 2020, pp. 167–184
37. Svantesson, D. J. B., *Article 3. Territorial scope*, in: Kuner, C.; Bygrave, Lee A.; Docksey, C., Drechsler, L. (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, Oxford, 2020, pp. 74 -100
38. Thon, M., *Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO*, *Rabels Zeitschrift für ausländisches und internationales Privatrecht / The Rabel Journal of Comparative and International Private Law*, Bd. 84, H. 1, 2020, pp. 24 – 61
39. Tzanou, M., *Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights*, in: Fabbrini, F.; Celeste, E.; Quinn, J., *Data Protection Beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, 2021, pp. 99. – 119
40. Van A.; Brendan; Koekoek, M., *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'*, *International Data Privacy Law*, Vol. 5, No. 2, 2015, pp. 105 – 120
41. Voss, W. G., *Cross-Border Data Flows, the GDPR, and Data Governance*, *Washington International Law Journal*, Vol. 29, No. 3, 2020, pp. 485 – 531
42. Vrbljanac, D., *Zaštita osobnih podataka i međunarodno privatno pravo*, in: Barbić, J. (ed.), *Međunarodno privatno pravo i globalni trendovi*, Hrvatska akademija znanosti i umjetnosti, Zagreb, pp. 127 – 155

43. Wilderspin, M., *Overriding mandatory provisions*, in: Basedow, J.; Rühl, G.; Ferrari, F.; de Miguel Asensio, P. (eds.), *Encyclopedia of Private International Law*, Volume 2, Edward Elgar, Cheltenham, 2017., pp. 1331 - 1336

EU REGULATIONS

1. 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 L 281
2. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177
3. 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 L 119
4. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689

GUIDELINES, REPORTS AND OPINIONS

1. WP29 2009: Article 29 Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, (WP 158, 11 February 2009)
2. EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, 12 November 2019
3. EDPS Response Cloud Act: European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex)' (10 July 2019)
4. EDPB, ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, Available at: [https://www.edps.europa.eu/sites/default/files/publication/19-07-10_edpb_edps_cloud-act_annex_en.pdf], Accessed 5 May 2026
5. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, (10 November 2020) (version for public consultation)
6. EDPB, Guidelines 02/2024 on Article 48 GDPR, Version 2.1, Adopted on 4 June 2025

CJEU CASE LAW

1. C-327/91, *French Republic v Commission* [1994] ECLI:EU:C:1994:305
2. C-381/98 *Ingmar GB* [2000] ECLI:EU:C:2000:605
3. Case C-101/01, *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596
4. C-131/12 *Google Spain* [2014] EU:C:2014:317
5. C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317
6. C-230/14 *Weltimmo* [2015] EU:C:2015:639
7. Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
8. C-191/15 *Verein für Konsumenteninformation* [2016] EU:C:2016:61
9. *Opinion 1/15* [2017] ECLI:EU:C:2017:59
10. C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] EU:C:2018:388
11. C-507/17 *Google Inc. vs CNIL* [2019] EU:C:2019:772
12. Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems* C-311/18, ECLI:EU:C:2019:1145
13. Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* [2020] ECLI:EU:C:2020:559