TERRITORIAL EXTENT OF THE GDPR: HOW AND WHEN EUROPEAN UNION LAW APPLIES TO NON-EU BUSINESSES

Venus Dutta, Symbiosis Law School, Pune, India

ABSTRACT

The GDPR, i.e., General Data Protection Regulation, is significant because of its wide-ranging territorial extent, which authorises European Union data protection legal framework to apply to businesses set up outside the EU. The GDPR withdraws from conventional territorial or regional rooted models of territory by embracing a practical outlook built in establishment, aiming, and the observation of EU individuals, through Article 3. The extraterritorial outstretch intents to avert administrative evasion and to secure a distinguished safeguard for personal data in an evolving globalised digital domain. Nevertheless, the width of the territorial extent of the GDPR elevates notable reasonable and legal concerns. Despite inadequate physical presence in the European Union, the non-EU businesses may be subject to large-scale acquiescence accountability, resulting in unreliability concerning the EU administrative authority limitations and GDPR's compatibility with international law standards. Thus, this article critically scrutinizes how and when the GDPR applies to non-EU businesses, examines the efficacy and authenticity of its extraterritorial scope, and contemplates if the present structure attains a suitable stability between robust data protection and legal reliability in trans-jurisdictional data processing.

Keywords: GDPR; European Union; Non-EU Business; EU data protection law.

1. Introduction

The GDPR, i.e., General Data Protection Regulation, constitutes a conclusive transference in the European Union's outlook to protection of data, most significant by means of its intentional outstretch surpassing the borders of EU. By permitting itself extraterritorial approach, the GDPR questions conventional, territorial confined perceptions of administrative jurisdiction and avers the European Union's traditional attitude in the worldwide digital economy. This wide-ranging territorial extent is not solely a practical characteristic of the Regulation, but also a deliberate strategic solution targeting at impeding non-EU businesses from avoiding EU data protection guidelines while maintaining profit from individuals' personal data within the EU.

The GDPR constitutes a practical rather than geographical scrutiny for applicability, through Article 3, emphasising on the aiming and observation of European Union individuals instead of physical locale of data processor or controller. While this perception nourishes the safeguarding of fundamental rights, it also uplifts notable concerns relating to legal reliability, proportionality, and applicability. Non-EU businesses may procure themselves subject to European Union law although having no physical presence in the EU, establishing tensity with standards of state autonomy and international jurisdiction.

Therefore, this article contends that despite the extraterritorial scope of GDPR is rationalised by the necessity to secure effectual and consistent data protection, its large-scale, and at times unspecified condition, risk applying inordinate compliance stress on non-EU actors and muddling trans-jurisdictional administrative applicability. By critically scrutinizing how and when EU data protection law applies to non-EU businesses, the article evaluates if the territorial reach of GDPR runs into a suitable stability between robust data protection and the authenticities of a globalised digital economy.

2. Historical Development of European Union Data Protection

In order to understand extraterritorial reach of the GDPR, the historical development of EU data protection law needs to be acknowledged.[1] Over the past five decennary, the European data protection has moved from a restricted regulatory concern into a fundamental rights-rooted legal scheme, demonstrating both technological advancements and the European Union's

[1] Malcolm Shaw, *International Law*, 9th Edition, Cambridge University Press, 2021, pp. 576–600.

traditional aims.

2.1 Early Substructures: Managerial and Regional Regulation

The emergence of the European Union data protection law date back to 1970s and 1980s, established by the elevation of computerised personal data processing and issues over violations of privacy:

- *Council of Europe Convention 108 (1981)* – It is the first binding international treaty that acknowledged computerised data processing, constituting guidelines like legality, motive limitation, and data standard. This instrument was fundamental in encouraging cross-border collaboration and harmonisation.

- *Directive 95/46/EC (1995)* – It is often known as the Data Protection Directive as it systematized EU-wide regulations for personal data processing, emphasising on harmonisation across the Member States while permitting resilience in enforcement.

2.2 Origination of Fundamental Rights Framework

The modification of the century pronounced a move from managerial protection to rights-based regulation:

- *Charter of Fundamental Rights of the EU (2000/2012)* – Article 8 acknowledges the right to the protection of personal data as a fundamental right, supplying a conventional foundation for robust European Union data protection.

- *Court of Justice of the European Union (CJEU) rulings* like Google Spain (C-131/12) and Digital Rights Ireland (C-293/12 and C-594/12), strengthened that personal data protection is not solely technological compliance but a key factor of human privacy, solemnity and autonomy.

2.3 The Digital Marketplace and Trans-jurisdictional Challenges

The restrictions of territorial regulation became apparent as digital technology and online marketplace advanced in the 2000s:

- *Trans-jurisdictional data flows* – Social networks, cloud computing and worldwide e-commerce indicates personal data oftentimes left European Union borders speedily.

- *Regional regulations and divisions* – Directive 95/46/EC permitted Member States adaptability, leading to uncertain applicability and compliance issues for multinational businesses.

- *Calls for betterment* – The European Commission focused on the requirement for a consistent, robust framing, effective in acknowledging global processing and developing technologies like AI, online tracking and behavioural profiling.

2.4 GDPR as the Climax of Historical Advancement

The GDPR (2016/679) demonstrates the climax of the historical route:

- Consolidation and Advancement – It superseded Directive 95/46/EC, establishing overarching rules, consistent enforcement across Member States, and systems to advance liability.

- Extraterritorial Targets – Article 3(1) and 3(2) incorporate the European Union's impact-based mechanism, focusing on the guideline that fundamental rights protection can outstretch beyond physical boundaries when EU citizen's data is affected.

- Impact of Historical Principles – Lawfulness, transparency, purpose restriction — are the key principles from previous directives that are maintained but now shaped as binding rights with undeviating enforcement, nourishing applicability opposed to non-EU actors.

- Context of Technology and Economy – GDPR's reach demonstrating the authenticities of the worldwide digital marketplace, acknowledging trans-jurisdictional data analysis, cloud storage and targeted online services.

2.5 Inferences for Non-EU Business

The historical development states why the GDPR enforces extraterritorially:

- European Union data protection is on no account only a local and regulatory issue, but

is a right-based, worldwide-intended legal structure.

- Despite inadequate physical presence in the EU, non-EU businesses are now core elements in a regulatory rights-based condition, emphasising on the progression from previous principles of liability and just to the developed extraterritorial environment.

- Comprehending the history aids in elucidating why certain ideas, i.e., monitoring, targeting and establishment, were incorporated, demonstrating a decade-long path aiming at protection of EU citizens in a growing digital world.

3. Research Gap

Non-EU businesses encounter unreliability in elucidating whether their pursuits establish "monitoring" or "targeting" of European Union individuals, specifically in the subjects of digital platforms, online services, and AI-based data analysis. The inadequacy of specific verge establishes compliance dangers, while engagement of a European Union representative and other liability commitments foists regulatory and economical concerns. Moreover, applicability across borders engages intricated relations with international law, state autonomy, and collaboration with third-country regulators, resulting in questioning about the viability and efficacy of extraterritorial management.

Such circumstances elevate critical tensity — the GDPR's extraterritorial enforcement targets at protecting the privacy rights of EU residents on a global scale, yet the legal unreliability and compliance issues encountered by non-EU businesses can obstruct innovation, contort trans-jurisdictional digital commerce, and constitute concerns over territorial authority. Hence, understanding the extent, limitations and applied inferences of GDPR's territorial scope is significant for legal scholars, policymakers, and multinational firms guiding the global digital commerce.

4. Research Questions

1. To what length does the framing of data protection as a fundamental right rationalise regulation that is impact-based for non-EU businesses?

2. What was the legislative objective behind the territorial reach of GDPR, and how does it balance between autonomy and extraterritorial applicability?

3. How does the international collaboration, territorial conflicts and regulatory intersection influence the applicability of GDPR against businesses outside the borders of EU?

4. How does the GDPR assist as a model for international data administration and impact global privacy structures?

5. Conceptual Substructures of Extraterritoriality in European Union Law

The GDPR's extraterritorial reach is needed to be understood within the large-scale framing of the EU territory and Public International Law. Therefore, the GDPR demonstrates a growing regulatory or administrative attitude, rather than portraying a quintessential deviation, in which territorial boundaries are no longer the only foundation for contending legal authority.[2] This development has been operated by trans-jurisdictional commerce activity, and to be precise, the borderless characteristic of digital data flows, which impacts individuals directly within the European Union, notwithstanding where processing occurs.

Conventionally, jurisdiction in International Law has been rooted in the principle of territoriality, where a nation operates comportment taking place within its physical borders. Previous data protection schemes imitated this model, connecting territory to locale of data processing or the constitution of the data controller. While this standard encouraged legal reliability and regard for state autonomy, it eventually became increasingly unsuccessful in the online marketplace. Multinational businesses could profit from the EU commerce while avoiding the regulations of EU by detecting activities of data processing outside the European Union, resulting in regulatory concerns and arbitrage.

The GDPR personifies a move toward impact-based regulation, in response, contending territory-based on the effect of activities on individuals in the European Union instead of physical presence. Article 3 of GDPR carries on accountabilities to non-EU actors that monitor or target individuals within the EU. This reach lines up with current practices of EU, specifically in competition law, where foreign activity is directed if is establishes suitable impacts within the internal market. By emphasising on impacts, the GDPR secures the efficacy of European Union data protection guidelines in the digital domain on a global scale.

[2] Orla Lynskey, The Foundations of EU Data Protection Law, Oxford University Press, 2015, pp. 117-142.

The ideological basis for this extension is additionally built up by the Union's acknowledgement of protection of data as a fundamental right as per Article 8 of the Charter of Fundamental Rights of the European Union.[3] From a rights-based viewpoint, restricting GDPR accountabilities to EU-instituted establishments would erode the successful safeguard of individuals. Thus, extraterritorial enforcement is rationalised as required to protect fundamental rights despite the fact where data processing takes place. Nevertheless, this attitude uplifts continuing issues related to legal reliability, proportionality, and possible disputes with other legal frameworks, focusing on the tensity between successful rights protection and conventional territorial principles.

6. Legal Structure of Article 3 of GDPR

Article 3 of the General Data Protection Regulation defines territorial extent of EU data protection law and lays out the legal foundation for its extraterritorial enforcement. It demonstrates a purposeful shift away from an absolute territorial replica of jurisdiction towards a standard that reports for trans-jurisdictional data processing and global online commerce.[4] The proviso elucidates when the GDPR is applicable and intends to avert non-EU organisations from eluding obligations of European Union data protection.

6.1 Objective of Article 3

The main purpose of Article 3 is to secure efficacy and consistent safeguard of personal data under the EU, despite the location of the controller or processor. It acknowledges regulatory concerns left by Directive 95/46/EC, where non-EU enterprises could avoid EU legal framework by processing data outside the EU. Furthermore, Article 3 intends to secure just competition by subjecting European Union and non-EU organisations in the same commerce to corresponding mechanisms.

6.2 Framework of Article 3

Article 3 constitutes 3 optional bases for the enforcement of GDPR:

- *Article 3(1)* enforces the GDPR to processing executed in the subject of a European

[3] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, Art 8.
[4] Paul De Hert and Michal Czerniawski, 'Expanding the Territorial Scope of EU Data Protection Law' (2016) 3 *International Data Privacy Law* 230.

Union businesses, regardless the location of where the processing itself takes place. The idea of "establishment" is stated widely to avert avoidance via offshoring or outsourcing.

- *Article 3(2)* enlarges the GDPR to non-EU processors or controllers that deliberately provide services or goods to individuals in the Union or observe their nature within the EU. This proviso demonstrates the GDPR's key extraterritorial system and is rooted on an impact-based attitude, which needing purposeful targeting to secure symmetry.

- *Article 3(3)* enforces the GDPR to European Union consular and sensitive missions in a foreign state in consonance with the Public International Law. Its reach in restricted and primarily supplementary.

These provisos function unassisted rather than cumulatively, corroborating broad exposure while securing ideological comprehensibility between impacts-based and establishment-based jurisdiction.

6.3 Legislative Purpose

Article 3's legislative aim portrays the European Union's reply to digitalisation and globalisation. Recitals 22-24 highlights a wide elucidation of establishment and clarify outstretching the GDPR to non-EU companies whose activities impact individuals in the Union. Beyond protection of individuals, Article 3 also demonstrates the aims of European Union to frame data protection approach on a global scale, while intending to balance extensive jurisdiction with legal reliability.

6.4 Case Law Analysis

1. *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*

   In the case of Google Spain (C-131/12), the CJEU held that the applicability of European Union data protection to Google Inc., a United States-based company, owing to the working of its Spanish subordinate.[5] Even though Google Spain did not conduct the data processing itself, its function in selling and encouraging commercial slot for

[5] Case C-131/12 *Google Spain SL and Google Inc v AEPD and Mario Costeja González* EU:C:2014:317.

the search engine was considered to be inextricably connected to the personal data's processing by Google Inc.

The Court focused on the fact that the processing was conducted in the subject of activities of the European Union construction, as commerce feasibility of the search engine relied on advertising income produced within the Union. This case constituted a powerful precedent for elucidating "establishment" as well as "in the context of" widely, highlighting practical and economic links over geographic or applied elements.

2. *Weltimmo S.R.O v. NAIH*

In the case of Weltimmo (C-230/14), the CJEU additionally explained the idea of establishment and held that a business registered in a specific Member State may be deemed to be established in another Member State if it provides efficacy and original activities there by means of firm arrangements.[6] In this case, a Slovak enterprise monitoring a website related to property, targeting Hungarian users, was discovered to have an establishment in Hungary owing to reasons like the usage of Hungarian Language, a representative of the common locality, and a Hungarian bank account.

The Court reasserted that nominal but authentic activity may serve to constitute jurisdiction, laying out if reflects a firm presence. This judgement strengthened the principle that establishment is evaluated on an authentic source, with focus on the originality of activities instead of formal registration.

7. Function and Responsibilities of Non-EU Processors and Controllers

As per Article 3 of GDPR, non-EU processors and controllers are bound to the Regulation whenever their activities related to processing fall within its extraterritorial extent. These accountabilities target at securing that the individuals' fundamental data safeguard rights in the EU are safeguarded, regardless of location of establishment of the processing entity.

7.1 Enforcement of Core Principles of GDPR

When Article 3 enforces, non-EU organisations are obligated by the core principles of GDPR

[6] Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2015:639.

and substantive guidelines. This engages adherence with principles in Articles 5 to 11, like fairness, lawfulness, data deprecation, transparency, purpose restriction, and security.

The primary implications are:

- *Lawful source for processing* – As per Article 6, non-EU companies must depend on of the six lawful bases of GDPR for all the activities related to processing that involves European Union data subjects.

- *Data subjects' rights* – Individuals' right to access (Article 15), right to rectification (Article 16), right to erasure (Article 17), right to restriction of processing (Article 18), right to portability (Article 20), and right to objection (Article 21) must be respected, irrespective of the geographic location of the controller.

- *Data protection by default and by design* – As per Article 25, non-EU businesses are supposed to combine privacy matters into processing operations and system designs.

7.2 Article 27 – Appointment of an EU Representative

In order to encourage applicability, Article 24 needs most non-EU processors and controllers subject to Article 3(2) to appoint a representative who is European Union-based. The representative caters as an interaction medium for administrative authority and data subjects, and provides assistance to matters related to compliance.[7] Restricted immunities are applicable for low-risk and occasional processing, but businesses involving in frequent or wide-ranging targeting individuals of the Union must acquiesce. Despite the absence of a European Union establishment, this necessity reinforces the extraterritorial applicability of GDPR by securing successful regulatory supervision.

8. GDPR's Enforcement Against Non-EU Businesses

Even though Article 3 of the GDPR outstretches European Union data protection law to non-Eu processors and controllers, applying these regulations beyond EU boundaries provides practical and legal concerns. Enforcement relies on the strengths of EU's supervisory

[7] Orla Lynskey, *The Right to Data Protection and Extraterritoriality*, *Common Market Law Review*, 53(1), 2016, pp. 143–172.

authorities, cross-border collaboration as well as the readiness of foreign businesses to comply.

8.1 Strengths of Supervisory Authorities

European Union's supervisory authorities have broad investigative and remedial strengths under the GDPR, which includes the capacity to ask for data, establish audits, issue orders of compliance, and direct regulatory fines that goes up to €20 million or 4% of the annual income on a global scale.[8] These strengths are formally enforced to non-EU entities, but their efficacy is oftentimes restricted by jurisdictional restraints out the borders of EU.

8.2 Cross-Border Enforcement Challenges

Actual enforcement issues involve restricted jurisdiction over foreign organisations, concerns in serving lawful documents, high resource pressures, and issues over the enforcement of Article 3.[9] Non-EU entities may challenge if their activities establish monitoring or targeting of individuals in the European Union, emphasising on the disparity between legal extent and applicability ability.

8.3 International Collaboration

In order to acknowledge these restrictions, the GDPR promotes collaboration with regulators of third-country by way of mutual cooperation, international agreements, and informal assistance. While these schemes encourage applicability, their effectiveness rely on collaboration by non-EU authorities and mutual adjustment amongst various legal systems.

8.4 Effect of Enforcement Actions

Famous cases against companies like Meta, Google, TikTok, WhatsApp, and Amazon, reflects the practical extraterritorial effect of GDPR. These activities have strengthened compliance inducements globally, and encouraged the "Brussels Effect", through which European Union data protection approaches increasingly encourage practices of global commerce.

9. Effect on Global Digital Marketplace and Innovation

The extraterritorial reach of GDPR has notably encouraged global online marketplace and

[8] GDPR, Articles 51–59, 83; European Data Protection Board, *Annual Report 2021*, Brussels, 2022, pp. 15–25.
[9] Peter Swire & Kenesa Ahmad, *International Data Privacy Law*, Vol. 5, Issue 2, 2015, pp. 113–127.

innovation by expanding European Union data protection approaches to non-EU entities.[10] This impacts trans-jurisdictional data flows, corporate schemes, and technological advancement globally.

9.1 Impacts on Cross-Border Data Flows

Non-EU businesses that monitor or target individuals in the Union must be in compliance with the GDPR, irrespective of location of data processing. This has reframed marketplace decisions on data processing and storage, specifically for online platforms and cloud services. Limitations on transfer of international data and plausibly reducing worldwide data-driven economy.

9.2 Consumer Trust and Compliance Cost

GDPR compliance directs substantial technical and regulatory costs, particularly on smaller businesses, and introduces businesses to the risk of considerable fines.[11] Nevertheless, compliance can also advance commerce reliability and consumer trust. GDPR-based enterprises may profit from unchallenging entry to commerce globally, because a lot of jurisdictions have embraced related data protection structures.

9.3 The Brussels Effect

The GDPR has given rise to a strong "Brussels Effect", promoting businesses to embrace European Union guidelines worldwide in order to lessen legal risk.[12] It has also encouraged the advancement of data protection laws globally. While the Regulation supports privacy-advancing innovation, it can establish challenges for smaller firms with restricted compliance resources, portraying its binary function as a rights-based as well as commerce-framing device.

10. Future Advancements and Betterment Debates

As the GDPR carries on with shaping worldwide data protection guidelines, the continuing debates highlights on developing comprehensibility, legal reliability, and flexibility, specifically relating to its extraterritorial enforcement. Policymakers, regulators, and courts

[10] : Daniel J. Solove, *Understanding Privacy*, Harvard University Press, 2008, pp. 300–320; European Commission, *Impact Assessment on GDPR*, 2012, pp. 45–55.
[11] Ibid; ENISA, *Privacy by Design in SMEs*, European Union Agency for Cybersecurity, 2020, pp. 12–18.
[12] Anu Bradford, 'The Brussels Effect' (2012) 107 *Northwestern University Law Review 1.*

have a vital function in framing the evolution of the Regulation.

10.1 Betterment and Interpretative Debates

Discussions on reform prioritises less on extensive amendments and more on comprehensibility. Offers engages comprehensible thresholds for monitoring and targeting, advanced direction for low-risk processing, and corresponding applicability to lessen pressures on smaller companies. Systematic comprehensibility by way of supervisory and jurisprudence guidance is majorly seen as the most probable route ahead.

10.2 Global Function of the GDPR

The GDPR carries on with serving as a model for international data administration. Its principles have encouraged data protection laws globally, and promoted worldwide embracement of EU-rooted standards by multinational businesses. Although it cannot supersede international agreements, the GDPR endures to be a primary source for harmonising privacy regulations and constructing digital regulation on a global scale.

11. Conclusion

The GDPR demonstrates a milestone in data protection regulation worldwide by means of its strengthened extraterritorial scope. By expanding its enforcement to non-EU processors and controllers under Article 3(1) and 3(2), the GDPR asserts that the data protection of citizens of the European Union and the fundamental rights to privacy are not restricted by borders of territory. Thus, the shift from normative territorial jurisdiction to an impact-based attitude portrays the actualities of a digital commerce described by cross-border data flows.

Non-EU businesses that monitor or target individuals in the Union, or performs though an establishment of EU, are completely subject to GDPR accountabilities, that includes compliance with key principles and obligatory necessities. The need to appoint a European Union representative under Article 27 encourages applicability, even though notable issues are present owing to jurisdictional limitations, legal unreliability, and obscurity that surrounds core ideologies like monitoring and targeting.

Regardless such concerns, the GDPR has had an evolutionary effect on a global scale, encouraging corporate practices and promoting similar legislation globally — the Brussels

Effect. Looking forward, subsisting advancement via regulatory guidance, case law, and aimed justification will be significant to balance successful rights safeguard with legal reliability and innovation. Hence, the GDPR is considered a strengthened example of EU's capacity to safeguard the rights of individuals while enhancing global approaches for data establishments in an evolving digital marketplace.

Bibliography

Primary Source

- Regulation (EU) 2016/679
- Directive 95/46/EC
- Charter of Fundamental Rights of the European Union [2012] C326/02

Secondary Sources

- Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (3rd edn, Oxford University Press 2020).
- Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
- Antonino Mantelero, *The Future of Data Protection: GDPR and Beyond* (Springer 2018).
- Graham Greenleaf, 'Global Data Privacy Laws 2023: Recent Developments and the "Brussels Effect"' (2023) *Privacy Laws & Business International Report.*
- Michael Finck, 'The Shaping of EU Data Protection Law: From Directive 95/46 to GDPR' (2018) 24 *European Law Journal* 94.