LUISS

Law, Digital Innovation and Sustainability

Cattedra Data Protetion Law

Jurisdictional Challenges of GDPR in Space: Data Protection and Cross-Border Transfers in Starlink's Satellite Network

Prof. Filiberto Brozzetti

RELATORE

Prof. Fabiana Di Porto

CORRELATORE

631553

CANDIDATO

Anno Academico 2024/2025

Contents

Chapter 1: Introduction

1.1 Background and Research

Internet access today is primarily delivered through terrestrial infrastructure: cables, fibreoptic networks, and mobile towers operated by national internet service providers (ISPs). These systems are physically embedded within national territories and regulated through established legal frameworks, both at the national and European levels. The flow of data across these infrastructures is typically confined to known routes, passing through domestic exchanges and transnational fibre-optic cables whose physical location and ownership are usually transparent to both operators and regulators. In such networks, data is transmitted through infrastructure located within defined jurisdictions, where national and European regulators have clear oversight. The application of data protection law in this environment is relatively straightforward: authorities know where data travels, which legal regime applies, and who is responsible for ensuring compliance. This structure enables regulators to conduct audits, investigate violations, and ensure that users' rights are upheld through mechanisms grounded in territorial jurisdiction.

This legal clarity begins to weaken when internet access is no longer tied to terrestrial infrastructure. Starlink, operated by SpaceX, is the most prominent example of a new form of internet delivery based on a network of low Earth orbit (LEO) satellites. Unlike traditional ISPs, Starlink does not rely on local cables or towers. Instead, users connect through a dish that communicates with satellites in orbit. These satellites then pass data to ground stations (physical gateways connected to the broader internet) or, in newer models, via inter-satellite laser links that relay data across space before it is downlinked elsewhere. The system is designed for global coverage, with thousands of satellites in low orbit creating a mesh-like architecture that enables uninterrupted service regardless of local infrastructure constraints. While this has significant practical benefits, it disrupts the underlying assumptions upon which current legal and regulatory systems are based.

At a technical level, this system allows users in rural or remote areas to connect where terrestrial infrastructure is absent or unreliable. The deployment of satellite internet services is often framed as a solution to the digital divide, enabling connectivity in geographic regions that lack traditional infrastructure. But from a legal perspective, it

introduces a fundamental uncertainty: where does user data go, and under whose jurisdiction does it fall? If a user in Italy sends or receives data via Starlink, it is not necessarily clear whether that data is transmitted through ground infrastructure located in the European Union (EU), or whether it is routed via a satellite connection to a ground station outside EU borders. This becomes even more difficult to assess as Starlink expands its use of satellite-to-satellite links, reducing reliance on fixed ground infrastructure altogether. When data is routed across multiple satellites before reaching the ground, the entire processing chain becomes decoupled from any specific jurisdiction. This "loss of knowledge of location" is increasingly typical of globalised data infrastructures, especially in networked environments where territorial touchpoints are bypassed entirely (Koops and Goodwin 2019, 9).

Starlink does not publicly disclose where user data is routed, nor does it provide any binding commitment that data from EU users remains within the Union. The absence of routing transparency inhibits any meaningful legal analysis of whether international data transfers have occurred. This lack of transparency matters under the General Data Protection Regulation (GDPR), which governs the processing of personal data and imposes specific requirements for transfers to third countries. Even if the content of user data is encrypted, the transmission paths and associated metadata, such as device identifiers, connection times, and IP addresses, are themselves considered personal data under the GDPR and fall within its scope. The regulation requires not only that data transfers be legally justified, but also that users are informed about how their data is processed and protected. Transparency is not a formal requirement but a precondition for the exercise of other rights, such as access, rectification, and objection.

This uncertainty is not merely theoretical. In February 2025, a parliamentary debate in Italy precisely raised these concerns. Lawmakers proposed restrictions on the use of foreign satellite networks, including Starlink, for sensitive communications. The discussion focused on the risk that data transmitted through satellite infrastructure operated by non-European entities might fall outside the reach of EU law, even if the services are used domestically. Although the proposed restrictions were ultimately withdrawn, the debate demonstrated that questions around data sovereignty, jurisdiction, and infrastructure control are moving from technical forums into national political

agendas. This signals a broader political realignment in how legal systems view network infrastructure: no longer as neutral or apolitical, but as vectors of strategic dependence. As Kuner notes, “the term ‘transfer’ is often used without being clearly defined, which creates difficulties in understanding the scope of regulatory regimes” (Kuner 2020, 28). This doctrinal ambiguity becomes critical when applied to hybrid systems like Starlink, where data flows are continuous, modular, and unclear. The challenge is not simply to decide whether a transfer has occurred, but whether the legal system can meaningfully apply its conceptual tools to systems that defy traditional models of flow, destination, and control.

The comparison often made between Starlink and conventional ISPs is misleading. While both provide internet connectivity, the architecture through which they operate is fundamentally different. National ISPs transmit data through networks located within their regulatory jurisdiction. Their infrastructure is accessible to oversight, and their data flows are governed by established protocols and domestic enforcement mechanisms. Compliance is tied to localisation: servers, switches, and cables are placed within territorial reach of enforcement authorities. Starlink, by contrast, operates through a distributed and borderless system where data flows are determined by satellite availability and network efficiency, not territorial boundaries. This decentralisation problem is not unique to Starlink. As Svantesson explains, “the mobility of data undermines the utility of several traditional jurisdictional anchor points” (Svantesson 2016, 3). Infrastructural decentralisation is increasingly characteristic of modern cloud and networked environments, but Starlink introduces a new form of jurisdictional dislocation: one in which even the controller may be unable to determine where data is processed or transferred.

The problem is not simply one of compliance in the narrow sense, but one of regulatory capacity. If data from EU users is routed outside the Union - whether to ground stations in third countries or through non-territorial satellite links - it is unclear whether current legal instruments under the GDPR are sufficient to ensure effective oversight. More importantly, neither users nor regulators have the tools to verify what happens to data once it enters this infrastructure. The GDPR is predicated on the idea that controllers must be able to demonstrate compliance, and that data subjects must be able to exercise their

rights. Without transparency and enforceable guarantees, the core principles of the GDPR, such as accountability, lawfulness, and data minimisation, risk being undermined. As Kuner remarks, “data may be routed through multiple countries without the knowledge or control of the data subject or even the data controller” (Kuner 2020, 29). This breaks the fundamental link between rights and enforceability upon which the GDPR is premised.

While Starlink serves as the primary case study, it is not an isolated example. Other satellite internet providers such as OneWeb (UK) and Amazon’s Kuiper project (US) are developing similarly decentralised orbital infrastructures. These systems also utilise LEO constellations with dynamically shifting transmission routes and ground station networks. Though they differ in deployment scale and legal domicile, the underlying architectural traits (extraterritorial routing, reliance on orbital interlinks, and non-transparent downlink logic) mirror many of the same challenges posed by Starlink. The findings in this thesis should therefore be understood not as company-specific, but as indicative of a broader shift in global communications infrastructure.

This thesis seeks to address that gap. It asks whether the GDPR, as currently structured, can adequately govern data processing in satellite-based networks, and whether the existing rules on international data transfers are suitable for an infrastructure that does not recognise national borders. The issue is not only whether Starlink complies with the law today, but whether the law itself can respond to a shift in how the internet is delivered and regulated. The objective is not to speculate on future technologies, but to interrogate the adequacy of current legal mechanisms in regulating already operational systems that fall structurally outside the territorial logic of the GDPR. As data processing moves into legally ambiguous terrain, “jurisdiction based solely on the territoriality principle is becoming less evident in the digital age” (de Hert and Czerniawski 2013, 1). As satellite networks become more prevalent and global connectivity becomes less dependent on terrestrial systems, this legal question will only become more urgent. The thesis situates Starlink not as a singular anomaly, but as a representative case study of broader infrastructural and regulatory trends that call for doctrinal clarity and systemic reform.

1.2 Objectives and Research Questions

This thesis, titled Jurisdictional Challenges of GDPR in Space: Data Protection and Cross-Border Transfers in Starlink's Satellite Network, explores how European data protection law applies to satellite-based internet infrastructure. The aim is to assess whether the GDPR is equipped to respond to the jurisdictional and enforcement challenges posed by decentralised, cross-border data routing in space-based networks. Starlink, operated by SpaceX, serves as the case study through which these broader questions are examined. Starlink is not selected as an outlier but as an emblematic example of a class of emerging technologies that call into question the effectiveness of law when infrastructure design subverts territorial logic. The focus, therefore, is not on the specifics of one company, but on how current regulatory tools interact with, and potentially fail against, novel technical configurations.

As outlined in the previous section, Starlink introduces a shift in the way internet services are delivered. Unlike traditional ISPs, which operate within clearly defined national jurisdictions, Starlink's infrastructure operates across borders and beyond territorial boundaries. This difference raises important legal questions about how data protection law, which is grounded in geographic concepts of control and oversight, can be applied to a network that does not follow the same logic. As Svantesson notes, “present thinking on jurisdiction is anchored in an unhelpful adherence to territoriality... it is often difficult to localise an event as occurring in a particular place in the online environment” (Svantesson 2016, 4). These challenges intensify when processing activities rely not just on global network routing, but on systems that operate entirely outside of conventional regulatory reach, such as satellites without national affiliation or downlinks that change dynamically. The regulatory model of territorial anchoring may thus no longer function when there is no consistent territorial link to enforce against.

The thesis does not set out to prove that Starlink is in breach of the GDPR. Rather, it asks whether the existing legal framework is structurally suited to a technological model that routes personal data through infrastructure that may fall outside the scope of European regulatory enforcement. In other words, it examines whether the GDPR can maintain its intended level of protection when applied to systems that are inherently transnational and

unclear in their data flows. This inquiry is especially pressing considering the erosion of jurisdictional clarity. As de Hert and Czerniawski observe, “the proposed EU General Data Protection Regulation (GDPR) goes beyond territoriality and bases its territorial scope on [a] destination approach” (de Hert and Czerniawski 2013, 230). Yet even this evolved model may struggle when faced with architectures that have no stable place of processing. These systemic problems are not merely legal abstractions; they represent tangible risks to the effectiveness of European data protection in real-world systems already operating at scale.

The objectives of this research are to:

- **Analyse the technical and legal characteristics of Starlink's infrastructure**, in order to understand how data is transmitted, routed, and potentially transferred across jurisdictions.
- **Examine the obligations that apply to such services under the GDPR**, particularly in relation to data transfers to third countries, user transparency, and controller responsibility.
- **Assess whether the nature of satellite-based infrastructure weakens the enforceability of GDPR standards**, either through jurisdictional gaps or through a lack of transparency and accountability; and
- **Propose policy responses or regulatory adaptations** that could strengthen GDPR compliance in the context of satellite internet services.

This approach is both interdisciplinary and problem-oriented. As Lydia Nkansah explains, “an interdisciplinary legal research method is defined as ‘legal research which incorporates insights from non-legal disciplines’... whereby a non-law data is added to black letter law for analysis to determine or form a perspective on law” (Nkansah 2016, 2). This method is not an academic luxury; it is a necessity when the phenomenon under analysis (satellite-based communication) is structured by both legal norms and technological constraints. Interdisciplinary work, however, must remain grounded in legal analysis. As Nkansah further argues, “an interdisciplinary legal research method should therefore begin with the aspect of the legal research methods... doctrinal research

to identify the pertinent law... before embarking on any empirical work on the policy or context" (Nkansah 2016, 11). This thesis therefore begins from law and remains rooted in legal method, even as it draws on technical insight to fully articulate the implications of space-based data infrastructure.

These objectives are translated into one central research question:

Can the GDPR, in its current form, provide effective protection for personal data processed through space-based internet services such as Starlink?

This core question is further explored through the following sub-questions

1. How does Starlink's technical infrastructure differ from that of traditional ISPs, and what implications does this have for jurisdiction and legal oversight?

2. To what extent can data routing through non-EU satellites or ground stations be considered a cross-border transfer under the GDPR?

3. Does the current regulatory framework allow users and data protection authorities to verify how and where data is processed in satellite-based networks?

4. What regulatory measures could improve transparency, legal accountability, and enforcement in the context of non-territorial internet infrastructure?

These questions form the structure of the thesis and guide the analysis across both technical and legal dimensions. They are designed not only to evaluate the sufficiency of current legal instruments, but also to identify areas where regulatory development may be necessary to address evolving forms of digital infrastructure. As Siems reminds us, "interdisciplinary research can lead to a more informed and more balanced judgment" when traditional doctrinal approaches prove too rigid or narrow to confront empirical complexity (Siems 2009, 6–7). This thesis therefore places itself deliberately at the intersection of law and technical systems, seeking not just doctrinal clarity but actionable insight. It treats the GDPR not as a static framework but as a living regulatory structure

whose application must be tested against technological shifts that were not foreseen at the time of its drafting.

1.3 Methodology and Structure

This thesis adopts an interdisciplinary approach, combining legal analysis with a technical understanding of internet infrastructure. The subject matter, data protection in satellite-based internet services, sits at the intersection of European data protection law and emerging communication technologies. The methodological choice to combine doctrinal legal reasoning with technical context reflects the nature of the problem: a legal framework, developed for terrestrial and relatively centralised data flows, is being tested against a decentralised and borderless infrastructure in which routing decisions are made without regard to jurisdictional boundaries. As such, the research draws on both doctrinal legal sources and publicly available technical descriptions of how Starlink's infrastructure operates in practice. The aim is not to treat these disciplines in parallel but to place them in active dialogue, allowing technical realities to reveal interpretive pressure points within the law.

At its foundation, the legal analysis is grounded in the General Data Protection Regulation (GDPR), with particular focus on its rules concerning cross-border data transfers, the scope of its territorial application, and the responsibilities placed on data controllers and processors. These legal provisions are not analysed in the abstract but in relation to how they function when confronted with technological conditions that disrupt their internal logic. Key regulatory concepts, such as "transfer," "establishment," and "appropriate safeguards", are evaluated in light of a system that obscures territoriality and defies infrastructural legibility. Case law from the Court of Justice of the European Union (CJEU), particularly the landmark decisions in Schrems II and Tele2 Sverige AB, forms part of the interpretative framework. These cases are not only doctrinally significant; they signal the increasing centrality of data transfer regulation in EU law and affirm the principle that data subjects must enjoy enforceable rights regardless of where their data is processed.

Guidance from the European Data Protection Board (EDPB), including Recommendations 01/2020 and Guidelines 03/2018, is also used to provide clarity on how core GDPR concepts should be understood in practice. These texts are particularly relevant when the law requires that controllers "map" data flows or implement "supplementary measures" to ensure equivalent protection in third countries. Where applicable, provisions from the ePrivacy Directive are considered, especially in relation to metadata and communication secrecy, both of which remain implicated in satellite-based services. The structure of this legal method aligns with Lydia Nkansah's suggestion that interdisciplinary research is most appropriate "if the study is about the external effectiveness of the law; that is, the external consistency of the legal system with the context and culture in which it functions" (Nkansah 2016, 5). That is precisely the aim here: to understand whether the GDPR, as an internally coherent system of rights and obligations, maintains that coherence when applied to infrastructures that undermine jurisdictional knowledge, user transparency, and regulatory control.

Alongside this legal foundation, the research engages with a variety of non-legal materials that are necessary to understand the technological environment within which personal data is processed. These include publicly available technical documentation (such as white papers, network diagrams, and regulatory filings), academic and industry literature on satellite internet systems, and reports by bodies such as ENISA and the European Commission. These sources are not treated as authoritative in the legal sense, but they offer crucial insight into how Starlink's infrastructure operates in practice. The aim is not to provide an engineering-level analysis, but to capture the key architectural features that have legal relevance. Particularly those that determine how, when, and where data is transmitted. Special attention is given to the implications of decentralised infrastructure and the potential for data to move across jurisdictions without user knowledge or meaningful control.

This analysis is not purely descriptive. The thesis seeks to identify the structural implications of decentralised infrastructure for legal compliance and enforcement. In this sense, the technical features of Starlink are not merely background but are integral to the legal argument. When, for instance, routing paths are determined algorithmically based

on network congestion and satellite availability, rather than user location or controller intention, this creates legal ambiguity about when a transfer has occurred or which regulatory regime applies. As Schrama (2011, 161) notes, “at least two different goals may be discerned” in interdisciplinary research: either to “give context to a legal problem or to test a specific legal approach as to its external effectiveness.” This thesis pursues both. On one level, it uses technical context to illuminate doctrinal ambiguity. On another, it tests whether the GDPR’s current legal framework can functionally govern data flows that are opaque by design.

The thesis does not rely on internal or proprietary data from Starlink, nor does it attempt to prove specific routing decisions in individual cases. Such an inquiry would fall outside the scope of what is feasible in a legal thesis and would require empirical access to data that is not publicly available. Instead, the focus is on analysing the structural conditions under which such routing decisions occur and assessing whether the GDPR provides sufficient legal tools for transparency, accountability, and enforcement. This analytical strategy acknowledges a methodological limitation that is well known in interdisciplinary legal research: “the legal researcher is very much dependent on datasets and information which are already available” (Schrama 2011, 161). The thesis works critically with this constraint by being transparent about its reliance on secondary sources and by focusing on the structural features of the system that are legally relevant, even in the absence of case-specific technical data.

In terms of legal method, the approach remains primarily doctrinal. Legal rules, case law, and regulatory texts are interpreted according to standard techniques of legal reasoning, including literal interpretation, systemic coherence, and teleological analysis. These are applied not in the abstract, but in direct response to the problems raised by the technical system under investigation. For instance, Article 44 of the GDPR is analysed not only by reference to its text, but also by questioning whether its conditions for lawful transfer, such as the ability to assess “essential equivalence”, can be fulfilled when the location of data processing is structurally unknowable. In this sense, the doctrinal method is informed by interdisciplinary awareness, but it does not abandon the rigour or internal logic of legal analysis.

The challenge of bridging law and technology is both substantive and methodological. As Siems (2009, 12) observes, the benefit of interdisciplinary legal research lies in its capacity to "gain a deeper understanding" and support "informed policy recommendation[s]." This is particularly relevant in fields where technological innovation rapidly outpaces legal development, leaving traditional doctrinal models ill-equipped to provide regulatory guidance. In such environments, doctrinal reasoning risks becoming either too abstract to be meaningful or too rigid to accommodate the dynamics of technical change. Rather than substitute empirical claims for legal reasoning, this thesis brings the two into a structured dialogue, aiming to ensure that legal interpretation remains grounded in both doctrinal clarity and contextual relevance.

The structure of the thesis follows the progression of the research question, moving from foundational context to applied legal analysis and then to forward-looking policy reflection. Chapter 2 reviews the relevant academic and regulatory literature on data protection and telecommunications law, with an emphasis on the legal uncertainties surrounding satellite infrastructure. It situates the thesis within existing debates about jurisdiction, accountability, and the limits of legal enforcement in globalised data environments. Chapter 3 sets out the technical and legal characteristics of Starlink's service, focusing on how its infrastructure diverges from traditional internet service providers and what consequences this has for regulatory oversight. Chapter 4 applies the GDPR to Starlink's model in detail, assessing the scope of its applicability (Article 3), the responsibilities of the service provider (Articles 4, 5, 13–22), and the enforceability of security and transfer provisions (Articles 32, 44–49). This chapter also integrates case law, EDPB guidance, and existing regulatory practices to show how and where enforcement breaks down.

Chapter 5 shifts from technical and legal analysis to structural critique. It identifies the risks posed by Starlink's infrastructure to both users and regulators, including the inability to trace data flows, the fragmentation of supervisory authority, and the failure of existing transfer mechanisms such as Standard Contractual Clauses within decentralised routing environments. It further demonstrates how the opacity of orbital infrastructure creates a space in which legal obligations under the GDPR cannot be operationalised, resulting in

a structurally induced zone of non-compliance. Chapter 6 responds to these challenges by outlining a three-part policy framework. It proposes the introduction of a new principle of infrastructural legibility under Article 5, requiring controllers to retain demonstrable knowledge of the environments and pathways through which personal data is processed. It further advocates for the creation of a mandatory Routing Disclosure Statement (RDS) for providers of satellite internet services, aimed at rendering routing practices visible to regulators. Finally, it examines the role of bilateral data embassies as jurisdictional fallback mechanisms where infrastructural control is technically or geographically infeasible. Chapter 7 concludes the thesis by synthesising the findings, reflecting on the structural fragility of enforcement under current law, and emphasising the political and legal urgency of adapting data protection regulation to an era in which connectivity is increasingly orbital, extraterritorial, and privately governed.

Chapter 2: Literature Review

2.1 Data Protection & Telecommunications

The evolution of telecommunications infrastructure is central to understanding the jurisdictional challenges posed by LEO satellite networks. Traditional internet delivery relied on terrestrial systems (cables, fibre-optic networks, and fixed ground stations) whose geographic location could be matched with legal authority. These systems formed the foundation for national regulatory control, as data transmitted through them could be traced, inspected, and governed by the laws of the country in which the infrastructure was located. This geographic correlation made it possible to identify both the actors responsible for data processing and the legal regimes under which they operated. Regulatory compliance, legal enforcement, and user redress were all structurally enabled by the fact that infrastructure and jurisdiction were physically and conceptually aligned.

Today, however, satellite constellations operate in near-Earth orbit, transmitting data through decentralised, extra-territorial systems that disrupt this alignment between infrastructure and jurisdiction. These new systems do not follow predictable, linear paths. Instead, they are optimised for speed, coverage, and performance, resulting in data being routed dynamically across moving nodes in orbit. As a result, the once-stable link between the place where data is transmitted and the law that applies to that transmission has become uncertain. This transformation marks a fundamental shift in the nature of global communications infrastructure.

Already in 1998, Joseph N. Pelton observed the disruptive potential of space-based communications: “By far the most significant change in coming decades is that space-based systems will increasingly deliver information directly to the consumer, rather than to a commercial data hub” (Pelton 1998, 81). This early insight identifies a shift away from traditional centralised data hubs, which were often located within specific jurisdictions and were thus subject to local regulation. As Pelton foresaw, the move to direct-to-consumer satellite transmission removes many of the fixed, traceable gateways through which data protection obligations were traditionally enforced. With this architectural change, enforcement mechanisms that rely on the ability to locate data or processing become significantly harder to apply. As these systems optimise for latency

and orbital coverage, “signals will zip back and forth to low orbits in hundredths of a second, a decisive advantage over the quarter of a second that data take to travel to and from GEO” (Pelton 1998, 81). This speed, while beneficial to users, undermines transparency and trackability for regulators.

Such technical developments have occurred alongside the globalisation of digital commerce. The internet has evolved into a medium not only for communication but also for global economic activity, and data is now a principal driver of value creation. As Kuner explains, international trade in data has grown rapidly in importance, both in terms of the amount of data flows and their financial value. In a more recent analysis, he notes that “the growing economic importance of data processing... has been estimated to be worth over USD 100 billion, and to be growing at almost 10% annually” (Kuner 2011, 11). The legal regulation of these flows becomes increasingly complex as the architecture of the internet no longer reflects the boundaries of legal systems. These flows no longer correspond to predictable, linear routes. Rather, “the architecture of the Internet means that even a transfer to a party in the same country may result in the message or file transiting via other countries, without the sender ever being aware of this” (Kuner 2011, 11). This phenomenon reflects a fundamental asymmetry: while legal regimes remain territorial, technical architectures are optimised globally. LEO satellite routing intensifies this disconnect, as data may be relayed through orbital links and downlinked to ground stations selected dynamically based on bandwidth or latency, not geography.

This infrastructural decoupling from territory presents a direct challenge to the regulatory ambitions of the General Data Protection Regulation. It creates an environment in which jurisdiction cannot be asserted with confidence, and legal obligations cannot be enforced reliably. As Voss notes, “Cross-border data flows have been described as commerce-enabling ‘hallmarks of 21st century globalization’” (Voss 2020, 488). These flows are essential to the modern digital economy, yet this globalisation has outpaced legal harmonisation. National data protection authorities cannot always coordinate across borders, and many jurisdictions lack the legal infrastructure to uphold standards comparable to the GDPR. This fragmentation is compounded when satellite infrastructure routes data beyond the reach of national oversight. Although “extraterritorial application exists and is being adopted in different areas of the world,” Voss observes that few legal

systems have frameworks as far-reaching as the GDPR (Voss 2020, 494). The GDPR is relatively unique in its ambition to project regulatory authority beyond EU borders, but this ambition is constrained when the infrastructure itself is non-territorial and unclear.

The result is a jurisdictional vacuum. Controllers may be unable to determine whether a transfer to a third country has occurred, and supervisory authorities may be unable to enforce obligations that depend on physical or legal presence. As Kuner puts it, “The regulation of transborder data flows focuses on policies like preventing circumvention of the law and guarding against data processing risks where the data are received” (Kuner 2011, 20). But in the case of orbital routing, these policies assume a level of transparency and control that is absent in LEO systems. These assumptions are no longer valid in an environment where infrastructure moves, is controlled remotely, and is governed by no single regulatory authority. The legal framework was not built to anticipate systems in which routing decisions are automated and infrastructure is mobile. As Kuner warns, “there is an inherent tension between the liberalisation of restrictions on the flow of capital and the use of transborder services on the one hand, and the regulation of transborder data flows on the other hand” (Kuner 2011, 26). Data flows, unlike capital, are rarely visible in real time, and often rely on highly complex backend architectures that defy localisation. Addressing this tension is urgent. As he concludes, “Ministers and government officials should grant international data flows the same attention as they do international flows of capital and international trade” (Kuner 2011, 29).

The problem is especially acute when data leaves Earth entirely. In this context, both regulatory oversight and enforcement become uncertain. Figg et al. describe how data protection enforcement becomes structurally difficult when infrastructure extends into space: “Our home-town gym may contract with a network of other gyms that span the globe, sharing our information across multiple continents and into outer space by transmitting the data via satellite” (Figg et al. 2019, 6). This metaphor illustrates how seemingly local interactions may rely on global infrastructure beyond user awareness. Users may be unaware that data is routed through orbital links, or that it is downlinked in third countries outside the European legal space. This introduces a layer of legal complexity and practical opacity that traditional regulatory models were not designed to manage. Given this complexity, the authors argue that “a new treaty, or new international

rules and/or regulations, should be considered addressing data protection laws in outer space" (Figg et al. 2019, 7). The suggestion of a new treaty reflects a broader consensus: current instruments, including the GDPR, struggle to govern data flows that are both invisible and untethered.

In summary, while global data protection literature has engaged deeply with the challenges of cross-border regulation, it has not yet adequately responded to the technical reality of satellite-based systems. Much of the existing work continues to assume a level of network legibility and geographic anchoring that no longer reflects technical realities. LEO constellations such as Starlink render core legal assumptions - territoriality, transparency, and enforceability - difficult to apply. This gap in governance reveals the need not only for doctrinal adaptation but also for cross-jurisdictional cooperation, technological oversight, and potentially new forms of international agreement. The legal system must now confront the possibility that its most powerful regulatory instruments fail precisely where they are most needed: in contexts where infrastructure is non-local, control is distributed, and data moves without borders.

2.2 GDPR Scope & Satellite Internet

The General Data Protection Regulation (GDPR) applies to personal data processing both within the European Union and, under certain conditions, beyond its borders. Two provisions define this scope: Article 3, which determines the Regulation's territorial reach, and Chapter V, which governs transfers of personal data to third countries. Together, these form the legal framework through which the GDPR seeks to ensure that the protection afforded to personal data within the Union continues when that data is processed elsewhere. However, the applicability of these provisions to satellite-based internet services such as Starlink remains uncertain, particularly where routing infrastructure disrupts conventional jurisdictional logic.

Article 3(1) applies to processing in the context of the activities of an establishment within the Union, while Article 3(2) extends this reach to non-EU entities that offer goods or services to, or monitor the behaviour of, data subjects in the Union. This destination-based model complements the traditional territorial approach and forms the basis for the

GDPR's extraterritorial application. De Hert and Czerniawski argue that "the GDPR complements a territoriality approach with a destination approach" (de Hert and Czerniawski 2013, 231), marking a deliberate shift from geographic presence to economic engagement as the trigger for jurisdiction. In doing so, the Regulation acknowledges that physical location alone is no longer sufficient to govern data flows in a digital environment. This development reflects the increasing complexity of modern data ecosystems, where companies may serve EU users without operating any physical infrastructure inside EU borders.

This shift, however, is not without controversy. As the same authors note, "the geographical scope of application of the new rules in the GDPR is already considered by some scholars as the most controversial aspect of the new Regulation" (de Hert and Czerniawski 2013, 231). The controversy stems in part from the legal uncertainty introduced by this approach. While the GDPR asserts authority over non-EU entities, the practical ability to enforce that authority often depends on infrastructure, cooperation, or the presence of a representative within the Union. The implications of this scope expansion become particularly complex when applied to decentralised satellite systems, where data processing infrastructure lacks fixed territorial ties. In such systems, the absence of an identifiable point of establishment or routing pathway makes it difficult to anchor legal obligations in space or geography. This raises questions about whether Article 3's conceptual reach is matched by real enforcement capacity.

While Article 3 establishes when the GDPR applies, Chapter V determines how it applies to international data transfers. This chapter introduces legal mechanisms designed to ensure that personal data retains its level of protection when transferred outside the EU. These mechanisms are meant to prevent a scenario where personal data, once processed outside the Union, loses its legal protections and becomes vulnerable to surveillance, misuse, or lack of accountability. Yet the definition of a "transfer" itself is far from clear. Kuner observes that "there is a lack of clarity as to the meaning of the term ['data transfer'], and regulatory instruments often use different ones without making it clear what they mean" (Kuner 2011, 11). This ambiguity is especially problematic in environments where data routing does not follow predictable geographic paths. Data may be sent to a ground station or satellite node located in a third country, or routed through

non-EU infrastructure without explicit instruction by the controller or knowledge of the user. Kuner further explains that “determining when a transfer has taken place is complicated by the fact that the Internet does not respect national borders” (Kuner 2011, 28). This observation highlights a fundamental tension between the territorial structure of legal systems and the borderless nature of digital data flows.

These complications are exacerbated in satellite internet systems, where data routing decisions are dynamic, automated, and often invisible to users and regulators alike. Routing is governed by algorithmic logic designed to optimise for latency, throughput, and network resilience, rather than jurisdictional awareness. As a result, data can be transmitted through multiple countries, or via satellite relays beyond national control, without any clear indication of where processing technically occurred. This unpredictability poses a serious challenge to regulators who must determine whether Chapter V is triggered, and if so, which safeguards are applicable. It also affects users, who are expected under the GDPR to be informed about where and how their personal data is handled yet have no way to verify the routing of their internet traffic through satellite-based infrastructure.

The European Data Protection Board (EDPB) Recommendations 01/2020 reinforce the obligation to maintain the GDPR’s standard of protection wherever personal data travels. These recommendations provide a six-step framework for exporters to assess third-country data transfers. Exporters are required to map data flows, evaluate the legal frameworks of third countries, and implement supplementary measures where necessary to ensure that the level of protection remains essentially equivalent to that provided within the EU. The idea is that the level of protection should follow the data, regardless of where it is routed or stored. If such measures cannot be applied effectively, exporters are advised to suspend or terminate the transfer. This approach presumes a level of routing transparency that is difficult to achieve in satellite internet systems. Controllers are expected to identify the countries involved, assess the potential for government access, and take mitigating steps. However, when routing decisions are not disclosed , or when data is relayed through orbital links that bypass terrestrial oversight, meeting these requirements becomes nearly impossible.

The requirement to “know your transfers,” as emphasised in the Recommendations, assumes that data flows are traceable and controllable, assumptions that do not hold when routing is determined by orbital link availability or dynamic network efficiency, as in Starlink’s infrastructure. This architectural opacity results in a compliance environment where even well-intentioned controllers may be unable to determine whether Chapter V is engaged. Moreover, because the GDPR does not explicitly define when an internal processing event becomes a cross-border transfer, controllers are left to interpret technical operations against vague legal criteria. This leads to regulatory uncertainty, inconsistent application, and a lack of enforcement clarity - all of which undermine the aims of both Article 3 and Chapter V.

The doctrinal relationship between Article 3 and Chapter V remains unsettled. Lu Yu highlights the lack of consensus on whether Chapter V applies to data flows from non-EU controllers already subject to GDPR under Article 3(2). This overlap introduces uncertainty in enforcement. While a non-EU entity such as Starlink may fall under the GDPR due to its targeting of EU users, whether its routing of data through third countries constitutes a “transfer” under Chapter V remains debated. The question is not simply academic; it affects the controller's obligations, the supervisory authority’s jurisdiction, and the data subject’s rights. Kuner reiterates that “the term ‘transfer’ is often used without being clearly defined, which creates difficulties in understanding the scope of regulatory regimes” (Kuner 2011, 28). This definitional gap is critical in the context of satellite internet, where the opacity of routing infrastructure makes it impossible to reliably identify when a transfer, in the legal sense, has occurred.

These overlapping provisions also reveal deeper enforcement challenges. Article 3 provides jurisdictional reach, but Chapter V offers the mechanisms for maintaining data protection across borders. This dual structure falters in environments where routing patterns are non-transparent or beyond the exporter’s control. The EDPB’s insistence on assessing the legal environment of third countries presupposes that exporters can determine where data flows. In LEO satellite networks, such as Starlink, this knowledge is absent. Routing decisions may bypass territorial checkpoints entirely, creating a structural gap between the GDPR’s legal scope and its enforceability. Without the ability

to localise a transfer or assess foreign legal frameworks, the required safeguards lose practical applicability.

In conclusion, while Article 3 offers a basis for applying the GDPR to satellite internet services that target EU users, and Chapter V outlines mechanisms for protecting data across borders, the intersection of these provisions is marked by doctrinal ambiguity and practical limitations. The lack of clear definitions, coupled with routing opacity in satellite systems, challenges the effectiveness of the GDPR's scope and safeguards in this context. This gap highlights the need for regulatory adaptation and greater scrutiny of how data protection obligations can be enforced over decentralised, extra-territorial infrastructures.

2.3 Key Research Gaps

The regulation of cross-border data flows has long been a central concern within data protection law. Foundational academic work has interrogated the jurisdictional challenges that global data processing introduces, but these analyses have remained tied to terrestrial infrastructures. Much of the legal and regulatory literature on this issue presumes that infrastructure is geographically anchored and that the physical location of servers, cables, or data centres corresponds in some way with the legal jurisdiction that governs them. This assumption, however, does not hold in the case of space-based internet systems, particularly low Earth orbit (LEO) satellite constellations, which operate across shifting orbital paths and non-territorial domains. These systems introduce a new dimension of complexity, one that has yet to be fully integrated into the doctrinal and regulatory discourse on cross-border data governance.

Kuner has consistently highlighted the lack of clarity surrounding the concept of "transfer" within the GDPR framework. He writes, "determining when a transfer has taken place is complicated by the fact that the Internet does not respect national borders" (Kuner 2011, 28). This definitional uncertainty persists across data protection scholarship and has not been resolved by judicial interpretation or regulatory guidance. While Kuner and others have explored how globalised infrastructures complicate jurisdictional boundaries, they remain focused on systems such as cloud computing and do not extend their analysis to the orbital data relays characteristic of LEO networks. The underlying

technical assumptions in these discussions tend to rely on systems that remain at least partially traceable: where routing paths, though complex, are still conceivable. Satellite internet infrastructure, in contrast, often lacks this basic traceability.

The same applies to Voss, who addresses the fragmentation of global data governance but limits his focus to terrestrial networks. As he notes, "a lack of international harmonization of law in the area results in rule overlap and rival standards" (Voss 2020, 486). This insight is highly relevant, as it identifies one of the structural challenges in applying legal frameworks like the GDPR across jurisdictions with conflicting or underdeveloped data protection regimes. Yet, this fragmentation becomes more acute when routing systems transcend not only state boundaries but also the Earth's surface, as in the case of Starlink's infrastructure. In such cases, the idea of overlapping rules becomes even more difficult to operationalise, because there may be no identifiable "place" to which rules can attach. The literature assumes some level of geographic correlation between infrastructure and legal oversight, an assumption that LEO satellite networks disrupt fundamentally. Legal regimes that require a point of jurisdictional contact struggle to engage with infrastructure that is fluid, shifting, and beyond the reach of domestic regulators.

The doctrinal scope of the GDPR itself, as framed by Article 3 and Chapter V, has been subject to substantial analysis. Scholars have explored how the GDPR aims to extend its jurisdiction based on both territorial presence and the targeting of EU data subjects. De Hert and Czerniawski frame this duality as an attempt to balance territoriality and destination-based targeting, noting that "the proposed EU General Data Protection Regulation (GDPR) goes beyond territoriality and bases its territorial scope on destination approach" (de Hert and Czerniawski 2013, 230). Their work highlights the GDPR's shift from jurisdiction based on physical presence to one based on economic interaction. Yet the interpretation of the territorial scope remains unsettled. Lu Yu highlights that "the interpretation of the territorial scope of Article 3 GDPR remains unsettled and continues to generate scholarly debate" (Lu Yu 2023). These debates are important in understanding how legal reach is asserted in a digital environment, but they are rooted in assumptions about stable infrastructure locations and clear legal oversight, therefore conditions that do

not exist in satellite-based routing environments. Orbital systems challenge the very foundation of legal interpretation by removing any consistent territorial anchor.

Further complicating the issue is the relationship between Article 3 and Chapter V. Lu Yu has examined this interaction within the context of China-EU data flows, noting the doctrinal overlap and uncertainty regarding whether non-EU controllers subject to Article 3(2) are also bound by Chapter V's transfer mechanisms. However, this analysis does not extend to non-terrestrial infrastructures, leaving a gap in understanding how GDPR safeguards apply to orbital data transfers. This omission is significant because it means that, even in sophisticated doctrinal discussions of jurisdiction and data transfer, the challenges posed by Starlink and similar systems are not addressed. While terrestrial and cloud systems may offer some level of visibility into data flows, space-based systems function in an environment where not only is the infrastructure unmapped, but the routing decisions themselves are non-transparent and dynamically allocated by algorithms beyond legal scrutiny.

The regulatory authorities have also addressed data transfers, particularly in light of the Schrems II judgment. The EDPB Recommendations 01/2020 stress the requirement for exporters to know their transfers and ensure essentially equivalent protection in third countries. However, this guidance presumes a level of transparency and control that is incompatible with the dynamic routing systems of LEO networks. In the case of satellite systems, exporters may have no knowledge of whether data is processed in a third country or what legal framework applies at the point of downlink. Similarly, EDPB 03/2018 clarifies the territorial scope under Article 3 GDPR, reinforcing that controllers and processors outside the Union must comply where they target or monitor EU data subjects. This scope may apply to Starlink in theory, but it is unclear how compliance can be demonstrated or enforced in practice. EDPB 05/2021 offers updated guidance on standard contractual clauses (SCCs) under Chapter V, but these mechanisms are ineffective when exporters cannot determine where data is processed or routed. SCCs presume the possibility of identifying a data recipient or location; a presumption that fails in orbital infrastructure.

The CJEU rulings in Schrems II and Tele2 Sverige AB provide further context for the limitations of data protection enforcement. Schrems II invalidated the EU-U.S. Privacy

Shield due to insufficient safeguards against third-country surveillance, while Tele2 Sverige AB ruled against indiscriminate retention of metadata by national authorities. Both decisions underscore the importance of essential equivalence and proportionality, yet neither addresses how these principles apply to infrastructures like Starlink, where routing decisions are opaque and infrastructure is extra-territorial. These cases demonstrate the Court's commitment to upholding data subject rights and limiting state surveillance, but they assume that the location of processing and the applicable legal regime can be identified. That assumption does not hold in LEO networks, where jurisdictional control is fundamentally obscured.

While the literature has robustly engaged with the theoretical and doctrinal elements of GDPR enforcement, it remains tethered to terrestrial infrastructures and assumes a level of routing transparency that no longer exists in satellite-based systems. The structural conditions of LEO satellite networks, including mobile infrastructure, dynamic routing, and non-territorial operation, challenge the doctrinal assumptions upon which enforcement depends. None of the academic or regulatory analyses fully addresses how data protection obligations can be enforced in environments where infrastructure defies territorial jurisdiction and routing paths are not disclosed. The EDPB's focus on mapping data flows and assessing third-country legal frameworks is ill-suited to LEO constellations, where neither users nor controllers may know where data is processed at any given moment. This renders standard compliance mechanisms difficult or impossible to apply, and leaves a critical enforcement vacuum.

This thesis addresses a critical blind spot in the existing scholarship: the regulatory implications of decentralised, space-based data routing infrastructures that undermine the jurisdictional logic of the GDPR. While prior literature has focused on cross-border data flows in terrestrial and cloud environments, it has not accounted for the opacity and non-territoriality inherent in satellite networks such as Starlink. By examining how the GDPR's territorial scope and transfer provisions operate, or fail to operate, when routing decisions are automated and infrastructure is orbital, this study offers a doctrinal and technical assessment of whether current legal mechanisms can maintain data protection standards in an era of decentralised internet delivery.

Chapter 3: Starlink vs. ISPs: A Legal and Technical Distinction

3.1 How Traditional ISPs Operate and Their GDPR Obligations

Traditional internet service providers (ISPs) deliver connectivity through terrestrial infrastructure that is both physically fixed and jurisdictionally bound. In this model, data transmission occurs through a system of fibre-optic cables, undersea connections, national internet exchange points, and local data centres. These physical components are deployed within clear territorial limits and are subject to national laws and regulatory oversight. The routing of data, while sometimes international, is typically predictable, traceable, and capable of being localised at multiple points. This allows both users and regulators to identify where data travels, who processes it, and which legal frameworks apply.

To understand this system more fully, it is important to recognise how data transmission occurs in terrestrial networks. When a user sends or receives data through a traditional ISP, that data is broken into packets and routed through a series of physical points (such as modems, routers, switches, and exchange nodes) until it reaches its destination. These points of transfer are embedded in physical space and fall under the regulatory scope of the countries in which they are located. Even when a cross-border connection is made, for example through undersea cables between EU and non-EU countries, the entry and exit points can be identified, and the infrastructure operators are subject to agreements, treaties, and legal obligations. This makes the system amenable to legal governance because the actors and pathways involved in data transmission are relatively stable and transparent.

In the context of the General Data Protection Regulation (GDPR), this localisation creates a strong foundation for enforceability. ISPs based within the European Union are considered data controllers or processors, depending on the nature of their services, and are thus subject to the Regulation's full suite of obligations. These include ensuring lawful processing (Article 6), upholding data subject rights (Chapter III), implementing appropriate technical and organisational measures (Article 32), and cooperating with supervisory authorities (Article 31). The GDPR's accountability principle (Article 5(2)) further requires ISPs to document and justify their processing activities, including how

and where personal data is transmitted or stored. These obligations are not theoretical. They form part of a structured compliance regime that includes internal record-keeping, privacy notices, data protection impact assessments, and external audits.

A key distinction of terrestrial ISPs lies in the visibility of their infrastructure. Network nodes, exchange points, and data centres are generally known and accessible to national regulators. These facilities are often physically visited and inspected by national supervisory authorities or independent auditors as part of routine oversight or compliance investigations. Moreover, ISPs in the EU are often required to register their data processing activities and provide detailed privacy policies that reflect the physical realities of their operations. This includes disclosing whether data is stored domestically, whether it is transmitted to third countries, and under what safeguards. This transparency facilitates compliance assessments, audits, and user redress mechanisms. It also supports a broader system of trust between users, service providers, and regulators. When personal data is transferred to third countries, these ISPs must follow the requirements of Chapter V GDPR, including the use of standard contractual clauses (SCCs), adequacy decisions, or binding corporate rules.

The availability of clear technical documentation and the accessibility of infrastructure make enforcement more than just a legal possibility - they make it a practical reality. Supervisory authorities can investigate how an ISP routes data, request internal logs, and cross-check compliance with stated policies. In turn, data subjects can lodge complaints, seek access to their data under Article 15, and initiate legal proceedings if their rights are violated. All of this is enabled by the fact that the ISP's data processing is both knowable and attributable: two characteristics that are increasingly difficult to find in decentralised systems.

In practice, many European ISPs implement data localisation strategies to limit cross-border transfers and simplify compliance. These strategies involve storing and processing data within the same jurisdiction as the user, thereby reducing the legal complexity associated with international transfers. For example, an ISP in Germany may retain customer metadata and communication logs on servers physically located within the country, under the exclusive control of German staff, thereby avoiding the need to implement SCCs or conduct transfer impact assessments. Even when international

routing is necessary, the pathways are sufficiently stable to allow for risk assessments and the application of supplementary safeguards as outlined in the European Data Protection Board's Recommendations 01/2020. The ability to map where data is going, and to identify the legal environment it enters, is foundational to the application of these safeguards.

ISPs also fall under sector-specific obligations set out in the ePrivacy Directive (2002/58/EC), which governs the confidentiality of communications and imposes restrictions on the processing of metadata. This includes requirements for obtaining user consent before accessing terminal equipment and limitations on data retention. Metadata, such as IP addresses, connection times, and location, is treated with particular sensitivity under EU law because of its potential to reveal patterns of behaviour and personal associations. The Court of Justice of the European Union (CJEU) has reinforced these protections in cases such as Tele2 Sverige AB, ruling against indiscriminate retention of metadata by national ISPs and affirming the principle of necessity and proportionality in data retention practices. In this case, the Court held that laws requiring general and indiscriminate retention of traffic and location data were incompatible with EU law, highlighting that such practices infringe on the right to privacy and data protection as guaranteed under the Charter of Fundamental Rights of the European Union.

What makes terrestrial ISPs particularly effective as subjects of regulation is their embeddedness in local legal systems. These entities are registered with national authorities, pay taxes in specific jurisdictions, and interact with users who are physically located in known places. Their technical and corporate identities are visible, stable, and subject to formal obligations. They must also engage with supervisory authorities in the context of data breach notification under Article 33 GDPR and cooperate in the event of complaints or legal challenges. This level of interaction supports both proactive and reactive oversight and ensures that data protection law functions not just as an aspirational framework, but as an enforceable legal regime.

From a compliance standpoint, traditional ISPs benefit from relatively stable infrastructures that enable the operationalisation of GDPR requirements. Risk assessments, data protection impact assessments, and international transfer evaluations can all be conducted with a high degree of certainty. Controllers and processors know

where their systems are located, which legal frameworks apply, and what contractual or organisational safeguards are needed to remain compliant. In this environment, regulatory obligations map fairly well onto technical realities.

In sum, traditional ISPs operate within a legally structured and technically transparent environment. Their infrastructure is static, their data flows can be mapped, and their processing activities are subject to regulatory scrutiny. This model enables effective application of GDPR provisions and supports the enforcement of user rights. Infrastructural traceability supports legal responsibility; transparency supports accountability; and territoriality supports enforcement. As a result, the regulatory apparatus built by the GDPR, including jurisdictional reach, lawful basis requirements, and cross-border safeguards, can be implemented and tested in practice.

The challenge, then, lies not in their compliance capacity, but in ensuring that emerging internet delivery models (such as satellite-based systems) can offer equivalent transparency and accountability. While terrestrial ISPs may face their own difficulties, including cybersecurity risks, commercial consolidation, or public interest disputes, they do not suffer from the structural opacity that defines satellite constellations like Starlink. In LEO systems, routing paths may be hidden even from the controller; data may be processed in a country that is never disclosed; and the legal framework that applies may be unknowable. These conditions stand in stark contrast to the traceability and transparency that define traditional ISPs and form the basis for GDPR enforcement in the terrestrial context.

3.2 How Starlink's Infrastructure and Data Flow Differ

Starlink, unlike conventional internet service providers (ISPs), operates through a decentralised, orbital infrastructure that challenges established expectations about how and where data is transmitted. While traditional ISPs rely on fixed, terrestrial routes (typically fibre-optic cables, local switching points, and data centres located within national boundaries), Starlink's architecture is designed to circumvent these territorial constraints. Its technical structure is composed of a growing constellation of low Earth orbit (LEO) satellites which relay user data dynamically between orbiting nodes before downlinking the information to ground stations. This model has significant implications

for the visibility, traceability, and legal categorisation of data flows under the General Data Protection Regulation (GDPR).

A typical Starlink connection begins when the user terminal (commonly referred to as a "dish") transmits an uplink signal to the nearest visible satellite overhead. The satellite may then pass the data across one or more inter-satellite laser links , a technology Starlink has begun deploying to reduce reliance on fixed terrestrial gateways. Once the data reaches a satellite with an appropriate ground station in range, it is downlinked to Earth and from there enters the broader internet. This path is not static: routing decisions are based on satellite availability, latency optimisation, and bandwidth considerations rather than geographic or legal constraints. The same outbound signal from a user in France could be relayed via a satellite over Germany one day and via a satellite over international waters the next. The introduction of optical interlinks further disrupts any clear mapping of jurisdiction, as data may remain within orbital systems longer before touching ground.

This routing architecture stands in sharp contrast to that of traditional ISPs, whose physical infrastructure is fixed and registered within specific jurisdictions. When a user connects through a national ISP, the location of switches, routers, and data centres is generally known and regulated. This allows data protection authorities to ascertain where data travels, where it is stored, and what domestic legal regimes apply. In such contexts, ISPs typically act either as controllers or processors, and are bound by clear transparency and accountability requirements under the GDPR. These duties are reinforced by the ePrivacy Directive and national telecom regulation, which impose obligations to safeguard both content and metadata. Importantly, national ISPs are also expected to retain data localisation policies and to cooperate with competent supervisory authorities when necessary.

In the case of Starlink, by contrast, the absence of fixed terrestrial routing points makes it nearly impossible to determine, in any given transmission, whether personal data has left the European Union. Although some Starlink ground stations are located within the EU, the growing use of laser interlinks means that even users in Europe may have their data routed through satellites that downlink in third countries. The opacity of these routing decisions is exacerbated by the fact that SpaceX does not publish real-time or even generalised information about which ground stations handle EU user traffic. Without such

disclosures, neither data subjects nor supervisory authorities can ascertain whether and when an international transfer, as defined under Chapter V of the GDPR, has occurred.

This operational opacity is not merely a technical by-product of innovation; it fundamentally disrupts the legal classification of data flows. As Kuner notes, technological complexity and the effort required to track data sent over the Internet means that it may no longer be feasible to differentiate between transborder data flows and those that do not cross national borders (Kuner 2011, 6). In such contexts, the conceptual clarity that GDPR provisions presume, particularly around identifying when a transfer has taken place, begins to collapse. Where routing decisions are automated and designed to optimise speed rather than comply with jurisdictional boundaries, as in Starlink's case, the distinction between domestic and cross-border data flows becomes effectively untraceable.

Moreover, the mirroring or fragmentation of data across multiple routes and jurisdictions challenges the definitional clarity of what constitutes a 'transfer'. The GDPR presupposes that personal data crosses a border in a manner that can be legally observed and regulated. Yet as Kuner further explains, "it is difficult to apply the concept of transfer to situations where data is mirrored or backed up across multiple jurisdictions simultaneously" (Kuner 2011, 32). Starlink's architecture decouples routing from jurisdictional mapping. As data flows become distributed across orbital paths and may be relayed through non-EU nodes, it becomes increasingly difficult - if not functionally impossible - to determine whether a data transmission has entered a third country legal regime. This undermines the viability of key GDPR safeguards, such as standard contractual clauses or adequacy decisions, which rely on identifiable endpoints.

The decentralised nature of Starlink's infrastructure also introduces a significant accountability gap. In terrestrial networks, legal obligations follow infrastructure: a server or cable located in France is subject to French law and can be audited or inspected accordingly. Starlink's orbital model lacks this tether. If a French user's data is routed via a satellite that downlinks in a country without adequate data protection safeguards, enforcement becomes nearly impossible without voluntary disclosures or full infrastructure transparency, neither of which are currently offered.

This disjunction raises particular challenges for the enforceability of data subject rights under the GDPR. Transparency obligations under Articles 13 and 14 require that users be informed where and how their data is processed. Similarly, Article 44 prohibits transfers to third countries unless appropriate safeguards are in place. Yet without knowledge of routing paths or confirmation of whether a downlink occurred within or outside the EU, these legal protections become abstract. The user cannot verify, and the controller cannot demonstrate, that compliance has been achieved. This not only risks breaching the principle of accountability (Article 5(2)), but also breaks the operational logic of the Regulation, which depends on the traceability of personal data across borders.

In short, Starlink's technical structure subverts the jurisdictional logic on which the GDPR relies. By moving data through a mobile, automated, and legally unclear routing system, it renders territorial concepts of regulation difficult to apply. While the Regulation does not prohibit innovation in network design, it does require that personal data remain subject to enforceable protection, a condition that becomes fragile when neither users nor regulators can determine the infrastructural path that data takes. The implications of this decentralisation are not limited to Starlink alone, but extend to all future systems that use similar orbital routing, suggesting a structural mismatch between current data protection law and emerging modes of internet delivery.

3.3 Jurisdictional Challenges Unique to Starlink

The decentralised structure of Starlink's infrastructure presents fundamental challenges to the jurisdictional assumptions underpinning the GDPR. Unlike traditional ISPs, which are embedded within national frameworks and whose operations can be localised with relative ease, Starlink's orbital system disperses data across borders and territories in ways that defy conventional regulatory logic. This section examines the implications of that architecture for legal jurisdiction, enforcement, and data subject rights.

In the traditional model of internet regulation, jurisdiction is established through identifiable infrastructure, legal entities with a fixed presence, or the location of the user. Starlink, however, undermines all three. Its infrastructure operates in space, beyond territorial borders. Its satellites orbit the Earth continuously, making brief and varying contact with ground stations in multiple countries. Users connect through terminals that

communicate directly with satellites, which in turn relay signals to ground infrastructure located wherever optimal conditions, and not legal certainty, dictate. The effect is a global, dynamic, and fragmented network in which the usual markers of regulatory competence are dissolved or rendered irrelevant. As a result, Starlink creates a legal grey zone in which the relationship between infrastructure and jurisdiction becomes uncertain.

One of the central difficulties lies in establishing which legal regime applies to the data transmitted through Starlink's network. Jurisdiction under the GDPR is anchored in either territorial presence (Article 3(1)) or targeting/data subject behaviour (Article 3(2)). Both bases presume a meaningful connection between the processing and a physical or economic presence within the Union. However, Starlink's use of dynamic inter-satellite routing obscures the point of processing to such a degree that territorial links become unreliable indicators of jurisdiction. It becomes practically impossible to determine where the processing occurred, especially when data may transit through a chain of satellites and be downlinked to a foreign ground station chosen on the basis of latency or bandwidth, not law.

As Svantesson observes, "there is an increasing use of infrastructure that either is not connected to any one territory or that exists in multiple territories simultaneously" (Svantesson 2015, 23). This spatial indeterminacy complicates efforts to enforce data protection obligations, particularly where personal data may traverse several regions without ever passing through a fixed legal checkpoint. For regulators, it means that standard enforcement mechanisms, grounded in the ability to identify the location of data and the actor processing it, are no longer reliable. For data subjects, it means that their rights under the GDPR may become ineffective, as enforcement requires knowledge of where and how data is processed.

Furthermore, effective jurisdiction depends not only on where data travels, but also on who has the capacity to access or control it. Jurisdiction is not merely spatial but also functional. Kuner points out that "often, the issue is not the location of the data per se, but rather who has access to it, which authorities can compel disclosure, and what safeguards apply" (Kuner 2011, 33). In other words, control matters more than geography. In the case of Starlink, neither users nor data protection authorities can reliably identify which entity has technical or legal control over data at each stage of

transmission. If the downlink occurs in a third country, local laws may permit access by foreign surveillance agencies, thereby undermining the level of protection considered essential under EU law.

This issue is particularly concerning given the opacity of data routing in LEO satellite systems. Unlike traditional ISPs, where logs and network maps may be audited, Starlink does not disclose where its satellites relay data, or which ground stations are used for specific user connections. A user in Belgium, for instance, may unknowingly have their traffic routed via a satellite that downlinks to a station in a non-EU country with weak privacy protections. The user has no visibility over this, nor does the data controller have an effective means of tracking or controlling the routing path. This routing ambiguity fundamentally weakens GDPR enforcement, which relies on the capacity to localise processing for both regulatory intervention and judicial redress.

The difficulty in defining jurisdiction is compounded by the challenge of determining when a transfer under Chapter V has occurred. Kuner explains that the application of transborder data flow regulation depends on there being a "data transfer" between two territorial jurisdictions, which presupposes the ability to determine when personal data have crossed national borders and thus what their location is at a specific point in time (Kuner 2011, 122). Starlink's orbital routing mechanisms, which operate independently of territorial boundaries, frustrate this requirement. If no stable ground infrastructure is involved, and routing choices change dynamically with satellite movement, then the regulatory assumption of a knowable transfer event collapses. The very concept of a transfer, which is foundational to Chapter V, becomes epistemologically unstable in this context.

This concern is reflected in the distinction between legal presence and remote access. As Kuner further notes, "in some cases, personal data never physically leaves a jurisdiction, but may still be accessed remotely, raising the question of whether this constitutes a data transfer" (Kuner 2011, 30). In the case of satellite systems like Starlink, this distinction is especially difficult to maintain. For example, data collected in the EU may remain technically stored within the Union, but if it is accessible to foreign entities via satellite or ground station integration, does this constitute a transfer? Starlink complicates this issue by enabling remote access to EU user data from outside the Union, either through

satellite relays or foreign ground stations. The ambiguity of such access undermines the effectiveness of GDPR safeguards, including the legal instruments designed to protect data once it moves beyond the EU's legal space.

Another challenge relates to how Starlink should be categorised under the GDPR. Article 4 of the Regulation distinguishes between controllers and processors, yet the complexity of Starlink's operational model renders this distinction unclear. As Kuner notes, "regulatory obligations differ based on whether the party is deemed to be a 'data controller'... or a 'data processor'... and there is considerable disagreement about what these terms mean in practice" (Kuner 2011, 18). The classification is not merely semantic - it determines the scope and nature of legal responsibilities. If Starlink merely facilitates transmission but does not determine the purposes and means of processing, it may argue it functions as a processor. However, its control over routing, infrastructure, and capacity management suggests a degree of functional agency that would align more closely with the role of a controller. This is especially relevant because decisions about how data is routed can have legal consequences, such as triggering Chapter V obligations or affecting user consent.

The absence of legal clarity on this point affects not only the attribution of responsibility but also the applicability of core GDPR obligations such as transparency, accountability, and security. If Starlink is deemed a controller, it must provide users with clear information about how their data is processed, where it travels, and what safeguards are in place. If it is a processor, those duties fall to another entity, which may not exist in any meaningful or identifiable sense in the satellite context. The result is a regulatory vacuum in which no actor can be held fully accountable for GDPR compliance.

Finally, the jurisdictional complexity of Starlink's system intersects with broader questions about international cooperation and legal legitimacy. Koops and Goodwin argue that in today's environment, "it is important to speak of a 'loss of knowledge of location' rather than a 'loss of location'" (Koops & Goodwin 2013, 9). This reframing reflects the reality that while data may still be anchored physically in space, its location is effectively unknowable to those responsible for compliance. The GDPR, however, is predicated on the assumption that location (and by extension, legal responsibility) can be

determined. When a location becomes epistemologically inaccessible, as in the case of Starlink, the foundational logic of territorial enforcement breaks down.

This is not simply a theoretical challenge. Enforcement depends on the ability of data protection authorities to exercise jurisdiction, conduct investigations, and compel compliance. If regulators cannot determine where data is processed, or which laws apply at each point of transmission, they cannot enforce the Regulation in a meaningful way. Nor can they ensure that data subjects have access to effective remedies, a core requirement under Schrems II. This leads to a situation in which users may be subject to the GDPR in theory, but lack any practical means of invoking its protections. In such a context, the legitimacy of the law itself may be called into question, as it fails to provide the safeguards it promises.

In sum, Starlink's infrastructure not only complicates the mapping of data flows but also challenges the very basis on which legal jurisdiction is claimed and exercised. The Regulation's core mechanisms for establishing responsibility, determining the applicable legal regime, and enforcing data subject rights are all strained by an infrastructural model that defies localisation. These are not marginal issues, but structural gaps that go to the heart of data protection law's effectiveness in a decentralised digital world. As the next chapter will show, this presents significant obstacles to the effective application of the GDPR to satellite-based services.

Chapter 4: GDPR Compliance in Satellite Internet

4.1 GDPR's Applicability

This section evaluates whether and how the General Data Protection Regulation (GDPR) applies to Starlink's decentralised satellite internet infrastructure. Specifically, it analyses the relevance of Article 3 GDPR, which defines the territorial scope of the Regulation, and assesses whether Starlink meets the criteria of either establishment in the Union (Article 3(1)) or the targeting of EU data subjects (Article 3(2)). The section also considers whether falling within the scope of Article 3 necessarily entails compliance with Chapter V on international data transfers. These inquiries are essential to determine the legal reach of the GDPR in relation to space-based infrastructure, where territoriality is technologically unclear and jurisdictional control is contested.

Under Article 3(1), the GDPR applies to personal data processing "in the context of the activities of an establishment of a controller or a processor in the Union." This provision anchors regulatory jurisdiction in the physical and legal presence of an entity within EU territory. The Court of Justice of the European Union (CJEU) has interpreted this notion of "establishment" broadly. In the landmark case Google Spain (C-131/12), the Court ruled that the presence of a sales subsidiary in a Member State (where its activities were inextricably linked to data processing) was sufficient to trigger the applicability of EU data protection law. This judgment introduced a functional reading of "establishment," whereby commercial operations within the EU could subject a non-EU data controller to GDPR obligations, even if the actual processing took place outside the Union.

Similarly, in Weltimmo (C-230/14), the Court found that even minimal and decentralised infrastructure could qualify as an establishment if it involved stable arrangements within the Union. There, the operation of a website directed at Hungarian residents by a company formally registered in another Member State was found to constitute an establishment, based on the nature of its operations and the presence of local representation. These cases confirm that the threshold for establishment does not require formal registration or a centralised legal presence; what matters is whether the processing of personal data is carried out "in the context" of EU-based activities.

In the case of Starlink, the relevant operator is SpaceX, a United States company with no publicly disclosed subsidiary within the European Union that acts as a data controller or processor for its internet service. While SpaceX has entered into contractual arrangements with EU consumers and ships user terminals to several EU Member States, it has not formally established a representative entity within the Union that exercises control over processing operations. Without such a presence, and without any evidence of stable or ongoing processing activity "in the context" of an EU-based establishment, Article 3(1) is unlikely to apply.

However, the analysis does not end there. Article 3(2) extends the Regulation to data controllers or processors not established in the Union where their processing activities relate to the offering of goods or services to individuals in the Union, or the monitoring of their behaviour. This provision reflects a shift in the jurisdictional logic of EU data protection law: rather than being grounded in physical location, it is grounded in the effect of processing on individuals located in the EU. As Lu Yu explains, "Art. 3(2) shows a shift towards the passive personality principle. It focuses more on the EU individuals rather than the territory of the EU" (Yu 2023, 39). This extraterritorial approach represents a deliberate legislative strategy to ensure that data subjects in the Union do not lose the protection of EU law merely because a service provider operates from abroad.

It is difficult to argue that Starlink does not offer services to individuals in the Union. The company operates an EU-facing website, conducts contractual transactions with European customers, and ships hardware to addresses across multiple Member States. Its payment and billing systems accommodate EU currencies and VAT rules. These actions clearly satisfy the test of Article 3(2)(a), as they constitute the deliberate offering of services to data subjects in the Union. The key consideration here is intention: if a foreign company makes its service available to users in the EU and tailors aspects of its offering, such as language, pricing, or delivery options, to the European market, then the GDPR applies. The Regulation does not require an express statement of intent; the totality of a company's commercial behaviour can be enough to trigger jurisdiction.

Moreover, the European Data Protection Board (EDPB) confirms this view in its Guidelines 03/2018: "Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection... and to establish... a level playing field... in a context of

worldwide data flows." This guidance underscores the GDPR's role in regulating global data markets, not just European institutions. In line with this approach, de Hert and Czerniawski write that the GDPR "complements a territoriality approach with a destination approach," which "requires a relatively strong connection between the action and EU territory" (2013, 230–231). The combination of EU-targeted marketing, fulfilment infrastructure, and technical operations that impact EU users is sufficient to meet this requirement in the case of Starlink.

This jurisdictional basis is further reinforced when one considers the nature of Starlink's data processing activities. The company does not merely sell hardware; it provides ongoing, real-time internet access, which entails the continuous processing of user metadata, identifiers, geolocation signals, and potentially content data. These activities have a sustained impact on the fundamental rights of EU data subjects and thus fall within the protective rationale of the Regulation. The GDPR is not limited to static processing but covers dynamic services that operate across borders, provided that they are targeted at individuals within the EU. In this sense, the nature of the service and not merely its point of sale, becomes crucial for determining jurisdiction.

Nevertheless, the applicability of Article 3(2) raises a further question: does such applicability automatically engage Chapter V GDPR, which governs international transfers of personal data to third countries? This question is particularly relevant in light of Starlink's infrastructure, which involves the dynamic routing of user data through satellites in low Earth orbit and through ground stations located in various jurisdictions, including non-EU countries. The Regulation provides limited clarity on this issue. Article 44 states: "Any transfer of personal data to a third country... shall take place only if... the conditions laid down in this Chapter are complied with..." However, it does not explicitly state whether these provisions apply to entities brought into scope only by virtue of Article 3(2).

Lu Yu identifies this as a doctrinal grey area. She writes, "Beyond the complexity of Art. 3 and Chapter V GDPR within themselves, it is also ambiguous how these two sets of rules interact with each other" (Yu 2023, 3). Elsewhere, she observes that "the wording of Chapter V is still so general that it leaves some more detailed issues open... The answer to these questions cannot be conducted from the wording of Chapter V" (Yu 2023, 69).

This suggests that even if a controller falls within the GDPR's territorial scope under Article 3(2), it remains unsettled whether that controller is subject to Chapter V's transfer mechanisms when data leaves the Union.

The implications of this ambiguity are not merely academic. Starlink's data routing mechanisms rely on orbital paths and satellite relays that make it extremely difficult to determine whether, when, and where a data transfer occurs. As Kuner writes, "It is difficult to apply the concept of transfer to situations where data is mirrored or backed up across multiple jurisdictions simultaneously" (Kuner 2011, 32). Such decentralised architectures challenge the foundational assumption of Chapter V; that a data controller can identify the moment a transfer occurs and apply the relevant safeguards. Starlink's architecture frustrates this by design.

Moreover, even assuming that Chapter V applies to Starlink via Article 3(2), compliance becomes operationally challenging. The transfer tools outlined in Chapter V, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or adequacy decisions, all presuppose that a controller can identify the jurisdiction in which data is processed and assess its legal environment. But in the case of Starlink, neither the controller nor the data subject may be able to identify the point of downlink or the location of processing at any given time. This undermines the very purpose of the transfer regime, which is to ensure that data retains its level of protection even when leaving the Union.

Compounding this problem is the enforcement gap created by technological and jurisdictional opacity. Yu notes that "the wide application scope of the GDPR per Art. 3 inherently has shortcomings in its enforceability, so that Art. 3 itself alone could not provide a satisfying protection level to the natural persons" (Yu 2023, 54). This is echoed by Kuner, who acknowledges that "the extraterritorial application of data protection law is now increasingly accepted," but warns that its practical effectiveness remains limited (Kuner 2011, 153). The lack of physical infrastructure within the EU, coupled with a lack of transparency about routing paths, severely limits the ability of European regulators to monitor compliance, conduct investigations, or impose corrective measures.

There is also an unresolved normative question at play: is it sufficient for the GDPR to assert jurisdiction over a foreign service provider merely because its processing affects

individuals in the EU? This question cuts to the heart of international law's traditional reliance on territoriality. As Yu remarks, "It must be asked whether the application of Art. 3 alone is sufficient to ensure an adequate level of protection... the answer to the above question probably has to be negative" (Yu 2023, 71). In other words, while the GDPR may claim regulatory reach, this reach may not be accompanied by the practical means to guarantee enforcement or compliance, especially in the case of services that rely on extra-terrestrial infrastructure.

In summary, Starlink clearly falls within the material and territorial scope of the GDPR through Article 3(2), given its active targeting of EU users. However, the consequences of this applicability remain contested. The interplay between Article 3 and Chapter V is doctrinally unsettled, and the practical enforcement of data protection obligations in the context of decentralised satellite networks is fraught with uncertainty. These problems are not unique to Starlink but reflect broader tensions in applying a territorially rooted legal framework to borderless digital infrastructure. As the thesis progresses, these findings will underpin the assessment of Starlink's role as a controller or processor (Section 4.2), and the applicability of transfer rules to its orbital data flows (Section 4.3). Together, these analyses will determine whether GDPR compliance is structurally feasible or legally aspirational in the context of low Earth orbit networks.

4.2 Data Processing and User Rights

The identification of the data protection responsibilities borne by Starlink depends on whether the service qualifies as a controller or processor within the meaning of the GDPR. This distinction is legally significant. Under Article 4(7), a controller is the natural or legal person who determines "the purposes and means of the processing of personal data," while a processor, under Article 4(8), acts "on behalf of" the controller and lacks discretion over core processing decisions. The classification shapes the allocation of duties under the Regulation, including obligations to inform users, ensure the exercise of rights, and implement safeguards for cross-border data transfers. Where these roles are not clearly understood or disclosed, the protection of data subjects under the GDPR becomes compromised at a structural level.

Starlink's technical and commercial design points toward the conclusion that it acts as a controller in the context of its EU-facing services. The company unilaterally determines the configuration and operation of the data processing infrastructure, including the routing of internet traffic, the storage and retention of usage data, and the contractual terms under which EU-based customers access the service. These decisions are neither outsourced nor directed by a third party. The infrastructure is owned, deployed, and controlled by the operator, and the service is offered directly to end users without the intermediation of another controller. Starlink does not present itself as a subcontracted processor acting under instruction, and there is no indication that its processing activities are contingent on the direction of another entity. The architecture of the service therefore satisfies both the purpose and means criteria under Article 4(7), situating Starlink squarely within the scope of a controller.

The EDPB has confirmed in its Guidelines 07/2020 that processors must not determine the purpose of processing and may only make limited decisions about non-essential technical or organisational matters. While the controller/processor distinction is frequently misunderstood in practice, it rests on the capacity to exercise decision-making authority. As Kuner has observed, "regulatory obligations differ based on whether the party is deemed to be a 'data controller'... or a 'data processor'... and there is considerable disagreement about what these terms mean in practice" (Kuner 2011, 18). However, where the purpose of processing (namely, the provision of broadband connectivity) and the means by which this is achieved, through proprietary satellite routing and user terminals, are set unilaterally by the operator, classification as a controller is uncontroversial.

A potential counterargument might suggest that Starlink, by virtue of merely transmitting data without engaging with its content, qualifies as a passive conduit and should thus be exempt from GDPR obligations under Article 2(2)(d) and the corresponding provisions of the ePrivacy Directive. This exemption, typically invoked in the context of telecommunications providers acting as mere transmitters of signals, excludes from scope entities "when providing publicly available electronic communications services in public communication networks in the Union." However, such an interpretation fails when applied to Starlink for two reasons. First, Starlink exercises autonomous control over both

the routing architecture and the operational conditions under which personal data is processed. Unlike neutral transmission services, it unilaterally determines the technical parameters that define how, where, and under what security conditions user data travels, including whether it is routed via orbital links or downlinked in third countries. Second, the scope of the exemption under Article 2(2)(d) has been interpreted narrowly by the CJEU, especially when the provider in question determines the "means" of processing in any meaningful way (see BEREC Guidelines and Tele2 Sverige AB). Therefore, the functional role that Starlink assumes (actively managing routing decisions and controlling the infrastructure through which personal data is processed) aligns more closely with the definition of a controller under Article 4(7) GDPR than with that of a neutral intermediary.

Once this designation is established, the corresponding responsibilities under the GDPR become extensive. Chief among them is the obligation of transparency under Articles 13 and 14, which require the controller to inform users, at the point of data collection, of the identity of the controller, the purposes of processing, the categories of personal data concerned, the recipients of the data, and whether the data will be transferred to third countries. Where such a transfer occurs, the controller must also indicate whether an adequacy decision exists or, if not, what safeguards are in place under Article 46. Yet, in Starlink's case, no such disclosures are currently available. The company does not publish jurisdiction-specific privacy documentation addressing the conditions under which data originating from EU users may be routed to or processed in third countries. Nor does it clarify the nature of any cross-border transfer mechanisms in place. In the absence of this information, users are unable to evaluate the risks associated with the processing of their data or to exercise their rights under the Regulation in an informed manner.

This exclusion is not a mere technicality. The GDPR's transparency obligations are not optional; they are the legal precondition for the exercise of user rights. Without access to the basic facts of processing - who processes the data, where it is processed, and under what legal conditions - rights such as access (Article 15), rectification (Article 16), erasure (Article 17), restriction (Article 18), and objection (Article 21) become effectively unenforceable. The right to data portability under Article 20, for instance, presupposes that the data subject can identify the controller and the categories of personal data being

processed. Similarly, the right to object to certain processing activities requires that users be aware of the existence and scope of such activities in the first place.

The opacity of Starlink's infrastructure further obstructs the exercise of these rights. Because the company does not publicly disclose which satellites or ground stations are involved in processing EU data, or whether data is downlinked in countries outside the EU's jurisdictional reach, data subjects are unable to determine whether their personal data is being transferred to third countries, and under what safeguards. The European Data Protection Board has emphasised that "data exporters must know their transfers" and must conduct transfer impact assessments to determine whether the destination country provides an adequate level of protection (EDPB 01/2020). In the case of Starlink, neither the controller nor the data subject has reliable access to this information, which undermines not only the principle of transparency but also the enforceability of rights under Chapter V.

The legal risks associated with this model are not hypothetical. In May 2023, the Irish Data Protection Commission issued a €1.2 billion fine against Meta Platforms Ireland for unlawfully transferring personal data of EU users to the United States. The decision followed a binding resolution by the EDPB, which found that Meta's use of standard contractual clauses (SCCs) and supplementary safeguards failed to compensate for the absence of an adequacy decision and did not ensure "essentially equivalent" protection under EU law. The data transfers were described as "systematic, repetitive, and continuous," and Meta was ordered to suspend further transfers and bring its operations into compliance.

The Meta Ireland case illustrates the centrality of controller accountability in the GDPR's enforcement framework. Even where an entity operates from within the Union and has extensive compliance structures in place, failure to ensure the legality of cross-border data flows can result in the highest levels of administrative sanction. In contrast to Meta, Starlink has no visible compliance infrastructure in the EU, no published transfer mechanisms, and no apparent engagement with the safeguards required under Chapter V. While Meta at least attempted to maintain legality through the adoption of SCCs, Starlink appears not to have adopted any such framework, nor has it disclosed the existence of a data protection officer or EU representative under Article 27.

The absence of public documentation on how and where data is processed also raises questions under Article 5(2), which sets out the accountability principle: “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1” of the GDPR’s core principles. The lawfulness, fairness, and transparency of processing cannot be presumed; they must be evidenced through policy documentation, technical safeguards, and responsive governance. A controller that is structurally incapable of mapping its own data flows or demonstrating the existence of legal safeguards in third countries fails the accountability test.

This regulatory deficit also impairs the effective operation of Article 22, which governs automated individual decision-making. Although Starlink’s routing architecture may not involve decisions that produce legal effects in the sense of traditional profiling, the use of automated infrastructure to determine bandwidth allocation, latency, or traffic shaping may produce significant effects for individual users. If these decisions are made without meaningful user input or transparency, they may trigger the protections of Article 22(1) and (3), which require the controller to implement appropriate safeguards and allow for human intervention. Yet, without transparency regarding how such decisions are taken, users cannot determine whether these rights apply or are being violated.

Lu Yu has drawn attention to the consequences of this systemic uncertainty. She argues that “the wide application scope of the GDPR per Art. 3 inherently has shortcomings in its enforceability” (Yu 2023, 54), especially where territorial and jurisdictional anchors are lacking. Yu further suggests that “it must be asked whether the application of Art. 3 alone is sufficient to ensure an adequate level of protection... the answer to the above question probably has to be negative” (Yu 2023, 71). If controllers fall within the GDPR’s material scope but are not subject to effective oversight or capable of demonstrating compliance, then the regulation’s protective function is compromised.

The result is a form of legal liminality. Starlink appears to be subject to the GDPR in principle, but in practice evades most of its enforceable obligations through infrastructural opacity and regulatory dislocation. The company’s operational control over the purposes and means of processing data, combined with its failure to comply with basic controller duties under Articles 13, 14, 27, and 44, places it in breach of several core provisions. The Meta case demonstrates that even established multinationals with a physical presence

in the EU cannot avoid accountability when controller responsibilities are not met. Starlink, by comparison, lacks even the basic mechanisms for regulatory visibility.

These structural limitations raise broader questions about the applicability of the GDPR to decentralised infrastructure. As the next section will examine, the failure to identify and control data routing pathways creates parallel deficiencies in relation to cross-border transfer safeguards and information security. Where the location of processing cannot be determined, and the controller cannot document its legal basis for transfer, the cumulative failure of compliance mechanisms renders the GDPR's protections ineffective.

4.3 Security & Cross-Border Transfers

The final legal dimension of applying the GDPR to satellite internet services concerns two interlinked problems: the enforceability of obligations relating to information security, and the lawfulness of data transfers across jurisdictional boundaries. The former is governed by Article 32 of the GDPR, which imposes a duty on data controllers and processors to implement technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data. The latter is addressed under Chapter V of the Regulation, which outlines the legal conditions for transferring personal data to third countries or international organisations. In terrestrial networks, these obligations are typically framed within infrastructures that are legally mapped, physically anchored, and operationally auditable. In orbital architectures such as Starlink's, however, the application of these safeguards is profoundly disrupted.

Article 32 requires controllers to evaluate the risks presented by data processing activities and implement appropriate technical and organisational measures to mitigate those risks. The term "appropriate" is risk-based and context-specific, requiring an assessment of the nature, scope, context and purposes of processing. Measures may include, among others: encryption and pseudonymisation; the ability to ensure the ongoing confidentiality, integrity, and resilience of processing systems; mechanisms for restoring availability in the event of an incident; and procedures for regularly testing the effectiveness of security controls. Critically, the provision imposes a forward-looking duty to anticipate and manage evolving threats to data systems. However, the enforceability of this obligation

rests on an assumption of system transparency: that the architecture of data routing is open to regulatory inspection and the application of security standards.

Starlink's orbital network architecture frustrates these assumptions. First, its data routing mechanisms are opaque to external observers. A typical data packet sent from a user terminal in an EU Member State is uplinked to a satellite and dynamically routed through multiple orbital nodes, potentially via inter-satellite laser links, before being downlinked to a ground station. At no point is the path pre-determined or publicly disclosed. Satellite availability, orbital positioning, latency optimisation, and local congestion all factor into routing decisions that are executed algorithmically, in real time. This dynamic system design, while optimal for performance, presents a critical barrier to Article 32 compliance: neither the data subject, the supervisory authority, nor potentially even the controller can accurately determine where the data is at any given moment, and whether it is protected by appropriate safeguards during each phase of transit.

The GDPR's own understanding of "appropriate measures" includes both technical controls (encryption, access restriction, logging) and organisational measures (internal policies, staff training, risk assessments). But many of these depend on a clear knowledge of where the data is transmitted and stored. In the case of Starlink, information such as whether a satellite relay involves a downlink in a third country, or whether the data is buffered in orbital memory, is not made available. ENISA, the European Union Agency for Cybersecurity, has flagged this as a systemic risk in LEO systems. In its 2024 report, it notes that "the physical remoteness and non-territorial operation of orbital nodes create serious gaps in auditability and compliance assurance" (ENISA 2024). The agency further highlights challenges in applying consistent cryptographic standards across global satellite networks, particularly where data relays span commercial, military, and hybrid-use platforms.

While Article 32 deals with data security in a general sense, the more specific concern of cross-border data transfers falls under Chapter V of the GDPR. Article 44 sets the overarching condition: any transfer to a third country may only occur if the level of protection afforded to the data remains essentially equivalent to that guaranteed by EU law. Article 45 allows transfers where the Commission has issued an adequacy decision regarding the recipient country; Article 46 permits transfers based on appropriate

safeguards, such as standard contractual clauses (SCCs) or binding corporate rules (BCRs); and Article 49 provides narrow derogations for specific situations, such as explicit consent or the performance of a contract.

Each of these pathways assumes a critical factual precondition: that the controller knows when and where a transfer takes place. This factual precondition is precisely what breaks down in the context of Starlink. Because routing paths are not disclosed, and are in any case highly variable, it is often impossible to determine whether a particular transmission involves a third country, let alone which third country. As Kuner has noted, "the application of transborder data flow regulation depends on there being a 'data transfer' between two territorial jurisdictions, which presupposes the ability to determine when personal data have crossed national borders and thus what their location is at a specific point in time" (Kuner 2011, 122). This presupposition no longer holds in orbital communication systems. Without the ability to identify a destination country, none of the legal mechanisms under Chapter V can be properly invoked or evaluated.

The EDPB, in its Recommendations 01/2020, has attempted to operationalise Chapter V compliance through a six-step roadmap. The steps include: identifying and mapping transfers; verifying the legal tools relied upon (e.g. SCCs, BCRs); assessing third-country laws and practices; implementing supplementary measures if necessary; taking procedural steps to implement safeguards; and regularly re-evaluating the transfer environment. This framework reflects the post-Schrems II enforcement logic, where adequacy is no longer presumed and controllers must proactively justify the lawfulness of cross-border data flows. However, as this thesis has already shown, Starlink's system design makes even the first step - mapping transfers - impossible. Without knowledge of whether and where data is transferred, the controller cannot assess recipient country law, cannot evaluate the effectiveness of SCCs, and cannot determine whether supplementary measures are needed.

The Schrems II judgment itself underscores the regulatory logic behind these requirements. The Court invalidated the Privacy Shield framework in part because it failed to guarantee effective judicial redress in the United States for EU data subjects. It held that adequacy must be substantive, not merely formal, and must include enforceable rights and remedies. Article 47 of the Charter of Fundamental Rights was used as the

normative baseline. The Court reaffirmed that the GDPR's system of international transfers depends not only on technical safeguards but also on the institutional conditions of the recipient jurisdiction. If a country lacks independent oversight bodies, data protection legislation, and accessible redress pathways, then no transfer may take place, regardless of whether the data is encrypted or anonymised.

This logic collapses in the case of orbital routing. Even if data were encrypted in transit, and even if Starlink adopted SCCs as a default legal instrument, the inability to identify the countries involved in each transfer renders any legal assessment meaningless. Encryption is not a substitute for enforceable rights; it is only one of several safeguards. Moreover, as Lu Yu rightly observes, "it must be asked whether the application of Art. 3 alone is sufficient to guarantee adequate protection... the answer to the above question probably has to be negative" (Yu 2023, 71). Where legal instruments are detached from territorial application, the accountability structure of the GDPR unravels.

Nor can Starlink plausibly rely on Article 49 derogations to justify its data flows. These derogations are intended for specific and exceptional situations: for instance, where a transfer is necessary for the performance of a contract at the data subject's request, or where explicit consent has been obtained. They are not designed to sustain repetitive, structural transfers, nor do they absolve the controller from the duty to inform the data subject of the nature and consequences of the transfer. In the context of satellite internet routing, which operates continuously and without user-level transparency, these derogations cannot meaningfully apply. The EDPB has repeatedly emphasised that reliance on Article 49 must be "strictly interpreted" and cannot be used to circumvent structural compliance obligations.

The GDPR's logic of legal certainty thus runs aground on Starlink's dynamic, opaque architecture. The enforcement difficulties this creates are further compounded by the lack of a clear jurisdictional nexus. While terrestrial controllers are generally subject to oversight by a designated data protection authority (DPA) within the Member State of their establishment, Starlink's infrastructure is geographically dislocated. Without a registered EU representative under Article 27, or a physical presence in any specific Member State, it is unclear which supervisory authority would have standing to initiate a complaint or conduct an investigation. The absence of such jurisdictional anchoring

reduces the practical enforceability of both Article 32 and Chapter V, as DPAs cannot audit, access, or sanction infrastructure that lies outside their control.

This regulatory asymmetry becomes more visible when contrasted with cloud infrastructure. Although cloud services may also involve cross-border processing, they are generally subject to identifiable legal contracts, registered controller-processor relationships, and designated EU establishments. Their data flows, while complex, can be documented and reviewed. Furthermore, major cloud providers such as AWS, Azure, and Google Cloud routinely publish their data residency options and allow clients to specify regions. Satellite routing, by contrast, evades such configurability. The decisions that determine data location are made automatically, based on orbital parameters and network demand. No option is offered to EU users to localise processing, and no commitment is made to ensure routing stays within the Union.

These difficulties are not abstract. ENISA has categorised satellite systems as “high exposure architectures,” especially vulnerable to supply chain compromise, denial-of-service attacks, and unauthorised ground station access. Moreover, the 2022 attack on the KA-SAT satellite service, which disrupted European connectivity at the start of the Russian invasion of Ukraine, has demonstrated that satellite links can be directly targeted in geopolitical conflicts. This reinforces the GDPR's expectation, under Article 32(1)(d), that security measures must be regularly tested and updated. Yet in orbital systems, software patches often require physical access to ground terminals or depend on remote uploads that may be delayed or interrupted. This inhibits rapid mitigation and makes real-time risk management unfeasible.

The NIS2 Directive attempts to address these systemic risks by imposing obligations on providers of essential services, including electronic communications. It requires entities to conduct risk assessments, document vulnerabilities, and notify authorities of major incidents. Starlink, despite its significant footprint in the EU connectivity market, does not appear to have declared itself under NIS2, nor is there evidence that it engages with the cybersecurity authorities in any Member State. This creates a dual gap: the provider falls outside both the direct enforcement jurisdiction of DPAs under the GDPR, and the supervisory jurisdiction of national NIS2 authorities. As a result, the regulatory

ecosystem is unable to respond to security or transfer breaches, even where legal obligations are triggered.

Finally, a comparative insight may be drawn from terrestrial data infrastructure. Submarine cables, which form the backbone of international internet traffic, are subject to formal intergovernmental agreements, including landing rights, jurisdictional registration, and security audits. Their operators must maintain contact points in each country where the cable lands and are subject to domestic regulation. This enables the lawful application of GDPR Chapter V rules: a controller transferring data via a cable can usually identify which countries the data passes through, which legal regimes apply, and whether any local interceptions or surveillance are possible. The same is true for fibre-optic terrestrial networks. In contrast, satellite routing offers no such visibility. It bypasses all border controls, both physical and regulatory, while still transmitting personal data between jurisdictions.

This lack of enforceable control over routing decisions challenges not only the operation of the GDPR, but its foundational logic. If data cannot be localised, transfers cannot be regulated. If transfers cannot be regulated, user rights under Articles 13, 14, and 15 are undermined. If enforcement cannot occur, then the accountability principle under Article 5(2) loses practical force. The result is not merely a gap in the Regulation's application, but a systemic limitation on its normative promise. As this chapter has shown, neither Article 32 nor Chapter V can function where routing decisions are technically unclear, legally untraceable, and structurally extra-territorial.

Chapter 5: Risks & Enforcement Challenges

5.1 Data Localisation & Jurisdiction

Chapter 4 established that Starlink's infrastructure and operations fall within the material and territorial scope of the General Data Protection Regulation (GDPR). The application of Article 3(2) was found to be satisfied, given Starlink's deliberate targeting of EU data subjects, and its engagement in continuous data processing across the Union. However, this conclusion that Starlink is in principle subject to the GDPR does not answer a more pressing and difficult question: can the GDPR be enforced in practice against an infrastructure model that defies localisation? It is this transition from theoretical applicability to functional enforceability that forms the basis of Chapter 5. Where Chapter 4 was concerned with legal classification and doctrinal thresholds, this chapter focuses on whether those classifications give rise to real-world accountability. In this section, the focus turns to one of the core problems of enforcement: the absence of territorial anchors in Starlink's infrastructure and the resulting breakdown of regulatory jurisdiction.

The GDPR is territorially rooted. Even its most expansive provisions such as Article 3(2), which extends the Regulation to non-EU entities, operate through concepts that are, at their foundation, geographically meaningful. Article 3(2)(a), for example, is triggered when a non-EU entity offers goods or services to individuals "in the Union," and Article 3(2)(b) similarly relies on the monitoring of behaviour "within the Union." Both formulations assume that it is possible to locate the relevant processing activities, the affected individuals, and the responsible actors in space. Without this spatial orientation, regulatory enforcement becomes unstable. As Koops and Goodwin suggest, "framing cyberspace as 'space' rather than as 'place' can make a difference in terms of thinking about solutions" (Koops & Goodwin, p. 12). The shift in conceptual framing matters: when spatial assumptions collapse, so too does the basis for assigning enforcement responsibility within conventional legal systems. As Catanzariti adds, "The nation state is no longer the relevant community for digital law because the linkage to territory is no longer strictly relevant to the digital phenomenon" (Catanzariti 2024, 73).

This loss of localisation poses a direct challenge to how jurisdiction is exercised in data protection law. Jurisdiction, in this context, depends not only on a controller's legal classification but on the ability of regulators to observe, audit, and intervene in the

processing of data. Starlink's use of inter-satellite links, automated orbital routing, and globally distributed ground stations prevents such oversight. Data transmitted from an EU user may be relayed across multiple satellites, with no fixed path, before being downlinked to a ground station in a third country chosen dynamically based on bandwidth availability or latency. These routing decisions are made in real time, without user awareness or controller-level configurability. As Svantesson writes, "our current focus on territoriality, driven as it is by national interest, is unsustainable... I am 'territoriality-agnostic', or perhaps even a 'territoriality-nihilist'" (Svantesson, p. 11). In such a system, the very notion of processing "within" or "outside" the Union becomes incoherent.

To illustrate this point, consider the case of a Starlink user based in Austria. The user initiates an online session through a Starlink terminal. At that moment, the request may be transmitted to the nearest available satellite overhead, which could hand off the signal to another satellite through a laser link connection. This inter-satellite relay is performed based not on jurisdictional considerations but on efficiency; the aim is to reach a ground station as quickly as possible. That ground station may be located in a country with no adequacy decision from the European Commission, or in a jurisdiction that has surveillance laws incompatible with EU fundamental rights standards. Yet at no point in this process is the user informed, nor does the controller necessarily have the ability to determine, where the data went or what legal regime it entered.

This scenario underscores the broader difficulty: effective enforcement under the GDPR is predicated on traceability. Regulators and users alike must be able to determine where personal data travels in order to assess compliance with applicable safeguards. Starlink's architecture denies this traceability. It creates what Kuner describes as a technical and legal opacity. "Although determining the location of cloud-stored data is not as impossible as some authors are suggesting, the cloud does compound the locatability problem of data even further" (Koops & Goodwin, p. 8). In the context of orbital networks, the locatability problem is not just compounded, but it becomes practically insurmountable.

This undermines the application of GDPR Article 44 and the entire logic of Chapter V, which presupposes the ability to identify when a personal data transfer to a third country occurs. While Chapter 4 examined the doctrinal uncertainty about whether Chapter V

applies to entities subject only to Article 3(2), this section explores a more practical concern: even if Chapter V applies, how can it be enforced in an environment where data transfer events are technically invisible? The legal framework depends on known, mappable transfers. Without the ability to locate data, or even infer its trajectory, no effective transfer safeguards can be applied.

This has serious consequences for the GDPR's internal logic. The Regulation relies on a spatial model of control, in which obligations follow the flow of data. Under Article 44, any transfer to a third country must be subject to adequacy decisions, appropriate safeguards, or specific derogations. However, none of these tools can be meaningfully applied unless the location of the transfer is known. The European Data Protection Board (EDPB) has reiterated this requirement in its Recommendations 01/2020, which impose a duty on data exporters to "know their transfers," map data flows, and assess the legal framework of each third country involved. But such a framework is premised on the traceability of transfers: a condition that does not exist in Starlink's orbital architecture.

Kuner's analysis of transfer ambiguity remains central to this problem: "Often, the issue is not the location of the data per se, but rather who has access to it, which authorities can compel disclosure, and what safeguards apply" (Kuner, p. 35). Starlink amplifies this issue by enabling a situation in which neither the controller nor the data subject (and certainly not the regulator) can determine access jurisdiction or the legal regime in effect at the point of downlink.

The implications are compounded when viewed from a compliance standpoint. Even a highly motivated data controller that wishes to comply with the GDPR may find itself incapable of fulfilling its duties if the infrastructure it relies upon cannot offer the visibility necessary to meet legal requirements. Article 32 of the GDPR requires the implementation of appropriate technical and organisational measures to ensure the security of processing, including the ability to ensure the confidentiality, integrity, availability, and resilience of systems. But when data flows are determined by orbital mechanics and bandwidth load balancing, and when routing logs are not disclosed, those technical measures become a matter of guesswork. As Hert and Czerniawski note, "With the development of the information society and ease of data transfers through the web, the territoriality principle seems to be becoming obsolete" (2013, p. 231). The GDPR's

enforcement framework becomes brittle the moment that technical uncertainty meets legal rigidity.

To clarify, the issue is not merely the controller's lack of knowledge, but their systemic inability to gain that knowledge. In many traditional processing environments, lack of compliance results from poor organisational practices, lack of training, or negligence. In the context of Starlink's infrastructure, the problem is infrastructural: the system itself does not allow for localisation. This places even conscientious controllers in a structurally non-compliant position. They cannot track transfers, they cannot map flows, and they cannot meaningfully apply Chapter V tools, even if they want to.

This infrastructural opacity not only frustrates enforcement but disables proactive compliance. Controllers are required to implement appropriate technical and organisational measures under Article 32 of the GDPR. These include the ability to monitor data flows, protect against unauthorised access, and ensure the confidentiality and integrity of personal data. But where data routing is determined algorithmically, and relayed via satellites outside of any fixed path, even a well-intentioned controller may be unable to fulfil these obligations.

The result is a paradox: a system that is subject to the law but not susceptible to its implementation. The GDPR can claim jurisdiction over Starlink, but it cannot oversee, verify, or meaningfully influence how data is handled once it enters the satellite network. The law functions in name, but not in practice. Enforcement becomes a theoretical ideal, not a reality. Jurisdiction exists only on paper, not in action.

The problem becomes even more acute when one considers the distribution of legal responsibilities across multiple actors. In a typical terrestrial ISP environment, each segment of the data path is operated by a known and locally registered entity. National DPAs can audit local ISPs, issue fines, or demand compliance plans. By contrast, in the Starlink model, the actors controlling transmission points may be unknown or based outside the Union. A satellite may relay EU data over a foreign jurisdiction, but the identity of the operator and the applicable law remain obscured. The user does not know, the controller cannot verify, and the regulator cannot intervene.

This problem is not purely technical. It reflects a deeper structural incompatibility between the design of orbital networks and the enforcement tools of data protection law. GDPR enforcement is built on the idea that location implies responsibility and that knowing where data is processed enables accountability. Starlink inverts this logic: it processes data in a way that resists localisation, and therefore escapes direct responsibility. Even the EU's broad assertion of extraterritoriality under Article 3(2) cannot resolve this issue if the infrastructure does not yield to spatial mapping.

Koops and Goodwin capture the theoretical implications of this with precision: the GDPR assumes that knowing the "where" of data will lead to knowing the "who", and from there, to legal enforcement. But if location is unknown or unknowable, responsibility becomes diffuse, and enforcement becomes aspirational. Regulatory power is reduced to a symbolic assertion, rather than a practical tool. This turns the GDPR from a functional legal regime into a declaratory one: it claims protection but cannot operationalise it. As Kuner summarises, "Jurisdictional claims mean little if they cannot be enforced" (Kuner 2011, 33).

This risk is not hypothetical. It is reflected in real-world limitations observed by data protection authorities themselves. The European Union Agency for Fundamental Rights (FRA) has reported that many DPAs lack the technical capacity, cross-border cooperation mechanisms, or institutional access needed to investigate complex international data flows. When infrastructure is decentralised and globally distributed, as in Starlink's case, these deficiencies become systemic. Supervisory authorities may be legally empowered, but they are operationally blind. Their jurisdictional competence ends at the boundary of their technical visibility.

In this context, efforts to localise data processing, whether through legal mandates, controller commitments, or user choice become futile. Starlink's infrastructure is not configured to honour territoriality. It is designed to optimise speed, redundancy, and global coverage, not compliance with national borders. Any attempt to impose localisation requirements on such a system without a technical enforcement mechanism is unlikely to succeed. As a result, users are placed in a position where they cannot know where their data travels, which legal regimes apply, or whether their rights are being respected.

In conclusion, the absence of data localisation in Starlink's infrastructure creates a jurisdictional void. The GDPR's enforcement model, which depends on the ability to identify processing locations and apply legal standards, accordingly, is rendered ineffective. While Chapter 4 demonstrated that Starlink falls within the scope of the GDPR, this section shows that the Regulation cannot be reliably enforced when the architecture of data transmission removes the spatial anchors upon which jurisdiction and accountability depend. The promise of protection becomes unmoored from the means of enforcement. This is not a failure of law in theory, but a breakdown of law in practice - one that fundamentally challenges the GDPR's ability to regulate satellite-based services. This enforcement gap does not reflect a lack of legal principle, but a vacuum of operational capacity. "The normative vacuum resulting from the absence of sovereignty does not equate to the absence of legal space, and the phenomenon of data transfers may even amplify the reflexive capacity of state sovereignty precisely through the sovereign vacuum of outer space" (Catanzariti 2022, 12)

5.2 Regulatory Arbitrage

While Chapter 4 clarified that Starlink falls within the material scope of the GDPR, and Chapter 5.1 established that enforcement based on localisation is practically impossible in orbital infrastructure, the problem does not stop at enforcement failure. This section argues that satellite internet providers such as Starlink operate in a legal environment where not only is enforcement structurally disabled, but the law itself can be tactically circumvented. Regulatory arbitrage occurs when private actors exploit legal ambiguity, jurisdictional fragmentation, or procedural inefficiencies to avoid or minimise regulatory obligations. This is not merely the result of bad faith. It is, more fundamentally, the product of a system that allows the substance of legal protection to be selectively disengaged, particularly when the data economy becomes unbound from territory. Starlink does not violate the GDPR in a formal sense. Instead, it operates at the limits of what the GDPR can actually reach. This subchapter demonstrates how strategic fragmentation of infrastructure, legal presence, and operational control enables a form of structural non-compliance that existing enforcement mechanisms are not equipped to address. This fragmentation severs not only legal presence but the functional jurisdiction of Member States. As Catanzariti writes, "Jurisdiction allows States to give effects to

sovereign independence. This is not sufficient in the realm of data government if not associated with the property of infrastructures" (Catanzariti 2022, 67).

One of the most important features of the GDPR is its broad territorial scope, codified in Article 3(2). The Regulation applies not only to entities established within the Union, but also to those outside the Union who offer goods or services to, or monitor the behaviour of, individuals within it. However, the expansive reach of Article 3(2) introduces a doctrinal paradox. While it brings non-EU entities into scope, it does so without offering new enforcement powers to Data Protection Authorities (DPAs) beyond Union borders. The Regulation presumes that legal jurisdiction is matched by institutional capacity. This presumption breaks down when the subject of regulation, in this case a space-based internet provider headquartered in the United States, does not maintain meaningful infrastructure, personnel, or decision-making processes within the territory of the Union. Even when Article 27 requires the appointment of an EU representative, the practical role of such a representative is extremely limited. They may serve as a point of contact, but they do not establish enforceable presence, nor do they hold operational authority over data processing.

The CJEU's ruling in Schrems II underscores how fragile this model becomes in practice. The judgment invalidated the EU–US Privacy Shield, in part, because data subjects had no access to "effective and enforceable" remedies under U.S. law. At paragraph 105, the Court emphasised that any third-country transfer mechanism must ensure protection that is "essentially equivalent" to that within the Union, and that such protection must be capable of being enforced in practice. Moreover, at paragraph 120, the Court reaffirmed that supervisory authorities must be empowered to suspend or prohibit data flows when the legal regime of the recipient country fails to offer adequate safeguards. These principles are foundational. But as Section 5.1 demonstrated, their application depends on conditions that cannot be met in the case of Starlink. Namely, the ability to determine where data is routed, where processing occurs, and which authority should intervene.

This leads to a core enforcement asymmetry. The GDPR asserts extraterritorial control, but that assertion is undermined by a fundamental structural weakness: the Union lacks coercive tools over actors who retain no operational footprint within its jurisdiction. In practice, this means that controllers outside the EU may be covered by the Regulation on

paper but remain shielded from meaningful scrutiny in reality. The difficulty is not only one of law, but of infrastructure. Starlink does not merely outsource processing to third countries: it decentralises processing to a system that actively evades territorial anchoring.

This is compounded by the institutional fragility of Article 27. The requirement that non-EU controllers or processors designate a representative within the Union is often misinterpreted as establishing a functional proxy for regulatory oversight. In practice, however, these representatives typically serve only as contact points, often without legal or operational control over data processing activities. They cannot bind the company to regulatory outcomes, nor are they in a position to implement compliance frameworks. As a result, Article 27 fails to provide a meaningful enforcement pathway. The company remains distant, the representative powerless, and the regulator left issuing guidance with no practical effect.

The European Data Protection Board (EDPB), in its Recommendations 01/2020 on supplementary measures, provides a six-step roadmap for exporters relying on Standard Contractual Clauses (SCCs) to transfer data to third countries. These steps include identifying and mapping all transfers, assessing the legal regime of the third country, and implementing "effective supplementary measures" to ensure essentially equivalent protection. Crucially, the EDPB states that if adequate protection cannot be ensured, the transfer must be suspended or terminated. But this framework is built upon the assumption that controllers and processors can accurately identify where data flows, what legal regimes apply, and how safeguards can be enforced. In the case of Starlink, none of these assumptions hold.

Starlink's infrastructure, which relies on dynamic satellite-to-satellite relays and global ground stations, cannot produce consistent or verifiable records of routing decisions. There is no fixed infrastructure within the Union, no pre-determined path for data transmission, and no stable point at which a supervisory authority could intervene. Moreover, the nature of orbital routing is such that two identically configured transmissions may take entirely different paths depending on satellite availability and network congestion. The GDPR's reliance on controller-level knowledge and responsibility becomes untenable under these conditions. As the EDPB itself

acknowledges, “effective supplementary measures” can only operate where exporters can “know their transfers”, a precondition Starlink’s architecture cannot satisfy.

This opacity is not merely a technical feature but becomes an instrument of legal advantage. Regulatory arbitrage thrives in environments where legal and physical infrastructures are misaligned. By locating its legal entities outside the EU, declining to establish a controlling presence within any Member State, and operating through infrastructure that defies localisation, Starlink creates a compliance structure that is difficult to penetrate. It is not that the company is ignoring the law; rather, the law lacks the necessary reach and tools to enforce itself.

Paraphrasing Kuner, enforcement authority tends to stop at the border. Where legal norms lack extraterritorial traction, and where data flows cannot be tracked with sufficient granularity, the likelihood of practical enforcement drops to near zero. DPAs may investigate, but they lack direct access to the systems in question. Even mutual legal assistance procedures which might theoretically enable cross-border investigation are slow, diplomatically sensitive, and inapplicable to routine compliance assessments. The GDPR’s model presumes a form of voluntary compliance, backed by a credible threat of sanctions. But that threat vanishes when companies are not reachable by enforcement mechanisms, either legally or physically.

The one-stop-shop mechanism of the GDPR, intended to streamline enforcement across the Union, compounds the problem. While it centralises investigation to a single lead authority typically based on the location of the company’s “main establishment”, it also restricts the ability of other DPAs to act unilaterally. In the case of Starlink, there is no identifiable “main establishment” in the Union. No Member State can claim local jurisdiction, and no DPA has a clear mandate to lead an investigation. In such cases, enforcement efforts can stall entirely, not because of disagreement among regulators, but because no regulator has standing to act.

This lack of regulatory standing is not a theoretical problem. It has manifested repeatedly in high-profile investigations involving major U.S.-based tech companies, particularly those nominally headquartered in Ireland. The Irish Data Protection Commission (DPC) has been criticised for years over delays in handling complex cross-border cases involving

Meta, TikTok, and Google. These delays are not merely procedural. They are structural, stemming from the DPC's limited resources and the inherently cautious, consultative nature of cross-border enforcement. As the European Parliament noted in its 2023 resolution, "divergences between national DPAs and procedural delays undermine the coherent application of the GDPR." In the Starlink context, these delays become paralysis. Without a lead authority, and without local jurisdiction, no investigation is likely to proceed.

The consequence is a compliance model based not on legal obligation, but on enforcement probability. Companies assess not only what the law requires, but what the institutional capacity of regulators allows. This is the core of regulatory arbitrage. When legal risk becomes a function of jurisdictional weakness, companies are incentivised to structure themselves accordingly. The GDPR's ambition to set a global benchmark for data protection becomes increasingly symbolic when powerful actors can position themselves just outside its reach.

This dynamic also explains why certain companies, despite being subject to repeated public scrutiny, continue to operate with limited friction. Starlink, by providing internet access directly to users without relying on local telecommunications providers, avoids entering traditional licensing regimes. In many Member States, Starlink operates under informal or lightly regulated conditions, often through consumer hardware sales and indirect resellers. This limits the administrative hooks through which regulators might demand compliance. By engaging users directly and processing data via externalised infrastructure, the company ensures that no single jurisdiction within the Union can effectively claim supervisory authority.

The EDPB's Recommendations 05/2021 on the use of SCCs further reinforce this limitation. While the Recommendations clarify the obligations of exporters and outline technical safeguards, including encryption, data minimisation, and logging, they place the burden squarely on the exporter to implement protections that guarantee effective rights. But this logic breaks down when the exporter has no visibility over routing decisions, and when the infrastructure operator (Starlink) retains full autonomy over how and where data is transmitted. The controller may remain legally responsible, but operationally

powerless. This disconnect erodes the foundation of accountability under Articles 5 and 24 of the GDPR.

The European Union Agency for Fundamental Rights (FRA) highlighted this structural problem in its 2024 enforcement landscape review. The FRA observed that "Data Protection Authorities across Member States often lack the resources, expertise, and cross-border mechanisms to engage with non-territorial infrastructure providers," particularly in the context of satellite-based communications and decentralised cloud services. The FRA further noted that regulatory gaps persist even when legal competence exists, due to the absence of technical access and institutional leverage. This reflects a broader institutional dilemma: the GDPR assumes both normative authority and practical enforceability. But when enforcement depends on infrastructure control, the assumption collapses.

Svantesson's critique of symbolic jurisdiction becomes particularly salient here. As he notes, it is common for regulatory frameworks to claim extraterritorial application as a matter of legal principle, even when those claims are unenforceable. These assertions serve important expressive purposes, but they do not result in practical compliance. In response, some regulators may resort to extraordinary measures, such as blocking services or mandating data localisation. Yet these approaches carry significant trade-offs: they may restrict user access, fragment the digital single market, and provoke diplomatic conflict. As a result, such "market-destroying" tools are used sparingly, if at all. In practice, regulators default to exhortation, not enforcement.

This default weakens the perceived legitimacy of the GDPR. When users learn that protections cannot be enforced, and when companies realise that non-compliance carries little risk, the regulatory regime begins to unravel. Rights become abstract; obligations become advisory. The law survives on paper, but not in practice. For satellite-based services, which are uniquely insulated from territorial enforcement, this erosion is especially acute.

In conclusion, regulatory arbitrage in the context of satellite internet providers like Starlink exposes not only the fragility of the GDPR's enforcement model, but the deeper mismatch between territorial law and extraterritorial infrastructure. The Regulation's

tools, namely Articles 3, 5, 27, 44–49, were never designed for actors who can engage EU markets without engaging EU law. As enforcement capacity collapses, so too does the law's deterrent power. Compliance becomes a function of corporate discretion, not legal design. If the GDPR is to fulfil its promise as a universal framework for data protection, it must reckon with the structural incentives that reward fragmentation, opacity, and institutional avoidance.

5.3 User Risks & Compliance Barriers

The preceding sections have demonstrated that Starlink's infrastructure undermines localisation and enables regulatory arbitrage through legal and technical opacity. This final part of the risk analysis turns to the lived consequence of such a system: the erosion of user rights. The General Data Protection Regulation (GDPR) is anchored in the principle that data subjects must retain meaningful control over their personal data, regardless of the geographic or infrastructural context in which processing occurs. Yet when applied to satellite-based internet services, the conditions required to exercise those rights collapse. Users are denied the knowledge necessary to understand how their data is processed, the tools required to contest that processing, and the institutional pathways to seek redress. This chapter argues that Starlink's operational model not only fails to comply with the GDPR but structurally disables user rights. It further demonstrates that even well-intentioned data controllers cannot comply with the Regulation's requirements due to the architectural opacity of decentralised orbital systems. In such an environment, the normative foundation of European data protection law (user agency, accountability, and enforceability) no longer holds.

The GDPR guarantees a suite of substantive and procedural rights to data subjects, including the right of access (Article 15), rectification (Article 16), erasure (Article 17), restriction of processing (Article 18), data portability (Article 20), and objection (Article 21). These rights depend on the existence of a knowable relationship between the user and the controller: who holds the data, where it is being processed, and under what legal safeguards. Starlink's model disrupts all three points of contact. The company does not disclose the routing paths of user data, the jurisdictions in which it is downlinked, or the legal instruments (if any) that apply to such transfers. As Kuner observes, "Data may be routed through multiple countries without the knowledge or control of the data subject or

even the data controller" (Kuner 2011, 29). This is not a marginal concern. Without such knowledge, users are functionally excluded from exercising the rights that define the GDPR as a user-centric regulation.

The right of access, as codified in Article 15, is the foundation upon which all other rights are built. It obliges controllers to provide information on whether personal data is being processed, and where possible, to identify the recipients or categories of recipients to whom the data has been disclosed. This presupposes that the controller has sufficient knowledge of data routing to answer such questions truthfully. In Starlink's infrastructure, routing decisions are dynamic, automated, and opaque. A signal sent from an EU-based user may be uplinked to one satellite, relayed across several orbital nodes, and downlinked in a third country all without user awareness or controller-level logging. Under these conditions, the access right becomes illusory. Without access, subsequent rights such as rectification, erasure, objection, or portability cannot be meaningfully asserted.

The problem deepens when we consider the GDPR's transparency obligations under Articles 13 and 14. Controllers are required to inform users, at the time of data collection, about the identity of the controller, the purposes of processing, the existence of data transfers, and the safeguards that apply to such transfers. In the context of Starlink, no such information is made available. The company does not publish jurisdiction-specific privacy documentation that clarifies whether EU user data is routed through or processed in third countries. Nor does it disclose whether those countries benefit from an adequacy decision under Article 45. The European Data Protection Board (EDPB) has made it explicit in its Recommendations 01/2020 that data exporters must "know their transfers," and that this obligation entails an affirmative duty to map data flows and assess legal regimes where processing occurs. Starlink's model makes such mapping impossible.

Koops and Goodwin's analysis of cloud computing underscores the relevance of architectural opacity to the enforcement of data protection rights. As they note, "the cloud does compound the locatability problem of data even further, not only through its feature of moving data around but also through complications such as layered services and... floating cloud centres" (Koops & Goodwin 2013, 8). While cloud infrastructure remains partially localisable and auditable, Starlink's orbital system intensifies this challenge to

the point of total dislocation. Users cannot determine whether their data has been routed beyond the EU, nor can they verify the legal regime under which that data is ultimately processed. The principle of transparency is thus rendered meaningless: users are formally granted a right that the system structurally denies.

The breakdown of transparency mechanisms has a cascading effect on user redress. Articles 77 through 79 of the GDPR provide data subjects with the right to lodge a complaint with a supervisory authority, seek judicial remedy, and obtain compensation for data protection violations. These rights require the existence of a competent supervisory authority, a local representative of the controller, and a legal environment in which remedies are enforceable. In Starlink's case, none of these components are in place. The company has no known establishment or Article 27 representative in the Union. It is not registered with any data protection authority, and no Member State has clear enforcement jurisdiction. The result is a legal vacuum in which users may formally hold rights but have no venue in which to exercise them.

This institutional breakdown was explicitly anticipated in Schrems II, where the CJEU held that "the appropriate safeguards, enforceable rights and effective legal remedies... must ensure that data subjects... are afforded a level of protection essentially equivalent to that guaranteed within the European Union" (para. 105). That standard cannot be met in an environment where no supervisory authority has standing, no court has jurisdiction, and no user can ascertain whether their data was subject to a third-country transfer. The Fundamental Rights Agency has reinforced this concern, noting that "data protection authorities across Member States often lack the resources, expertise, and cross-border mechanisms to engage with non-territorial infrastructure providers." This institutional fragility does not merely limit enforcement; it invalidates the promise of legal protection.

Even if a controller were inclined to comply with the GDPR in good faith, the structure of Starlink's infrastructure makes such compliance unworkable. Chapter V of the GDPR regulates international transfers of personal data, requiring controllers to implement adequate safeguards such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). However, the applicability of these safeguards depends on the ability to identify the jurisdiction to which data is transferred. As Kuner states, "The application of transborder data flow regulation depends on there being a 'data transfer' between two

territorial jurisdictions, which presupposes the ability to determine when personal data have crossed national borders and thus what their location is at a specific point in time" (Kuner 2011, 122). Starlink's routing logic does not permit this determination. As a result, it is not only non-compliant but non-compliance proofed.

Moreover, the difficulty in applying GDPR transfer rules is compounded by the lack of a shared definition of "transfer" across jurisdictions. As Kuner further notes, "There is a lack of international consensus as to what constitutes a transfer of data, and definitions may vary significantly" (Kuner 2011, 31). This legal ambiguity reinforces the structural impossibility of compliance. Even assuming a controller is able to identify a downlink in a third country, it may remain unclear whether this counts as a transfer under EU law. The controller is thus placed in a state of legal limbo; responsible for obligations it cannot fulfil, and subject to standards it cannot interpret consistently across legal systems.

This loss of enforceable rights is not limited to Starlink. It represents a broader challenge for any decentralised, dynamic infrastructure that routes data without jurisdictional awareness. Comparable concerns have been raised in relation to blockchain networks and unregulated cloud environments, where data may be replicated across multiple nodes without any single point of legal accountability. These architectures, like Starlink's, operate according to principles of redundancy and efficiency, not legal traceability. In each case, the GDPR's logic of controller responsibility and user empowerment breaks down when applied to systems that are not only transnational but extra-jurisdictional by design.

By contrast, traditional ISPs are embedded within national jurisdictions. Their data routing paths are visible, their processing infrastructure is registered, and their data protection compliance can be verified. They appoint local Data Protection Officers, maintain Article 30 records of processing activities, and can be held to account by national supervisory authorities. The same user in the same jurisdiction enjoys materially different protection depending on whether they use a terrestrial or satellite-based service. This is not a reflection of user choice or consent, but of regulatory reach and infrastructural visibility. Such a disparity raises normative questions about the legitimacy of legal guarantees that are enforceable only in infrastructurally convenient contexts.

The cumulative result of these deficits is the effective dismantling of data subject protection in the context of satellite-based internet. The GDPR's model depends on three pillars: transparency, accountability, and redress. When all three are removed, the Regulation becomes symbolic. Users believe themselves protected under Union law, yet face an ecosystem that offers no information, no remedy, and no access. The system thus ceases to function as law. As Kuner reminds us, "Jurisdictional claims mean little if they cannot be enforced" (Kuner 2011, 35). Legal provisions that exist only on paper may serve a declaratory purpose, but they fail to meet the standard of protection that the GDPR aspires to deliver.

This chapter has demonstrated that the failure of the GDPR in the context of satellite-based services is not limited to theoretical enforcement or doctrinal uncertainty. It extends to the practical experience of users who are denied both the means and the venues to assert their rights. Without infrastructural transparency, jurisdictional anchors, or regulatory access, the GDPR's protections remain structurally inaccessible. The following chapter will consider how this reality can be addressed through legal reform and institutional innovation. If the European legal order is to remain credible, it must respond to the emergence of infrastructures that elude its foundational assumptions.

Chapter 6: Policy Recommendations

6.1 Reforming Article 5: Embedding Infrastructure-Based Accountability

The preceding chapters have demonstrated that the General Data Protection Regulation (GDPR), while ambitious in its territorial reach and structural design, faces a fundamental challenge when applied to decentralised, opaque infrastructures such as Starlink. These systems operate outside traditional jurisdictional logic, with data routed through orbital relays and foreign ground stations based on efficiency metrics rather than legal parameters. As shown throughout this thesis, the consequence is not only a gap in enforcement, but a collapse in the very preconditions that enable legal compliance. If neither the user, the controller, nor the supervisory authority can identify where personal data is routed or processed, then the foundational principles of the GDPR become legally ineffective. The task of this section is to propose a concrete and legally actionable reform of the Regulation, specifically, a revision to Article 5 that would restore enforceability by embedding infrastructural legibility as a core data protection obligation.

Article 5 of the GDPR is the normative spine of the Regulation. It sets out the core principles governing the processing of personal data: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and, under Article 5(2), accountability. These principles are not optional. They form the basis upon which all other rights and obligations are constructed. Without them, the Regulation loses coherence. However, as demonstrated in Chapters 3, 4 and 5, these principles become unenforceable in the context of satellite-based internet infrastructure where routing decisions are automated, non-transparent, and often unknowable.

The proposed reform to Article 5 is therefore not intended as a doctrinal innovation, but as a practical corrective. It addresses a specific structural gap exposed by Starlink and similar systems: the inability of controllers to trace, document, or disclose the movement of personal data through their infrastructure. This gap directly undermines compliance

with transparency (Art. 5(1)(a)), purpose limitation (Art. 5(1)(b)), and accountability (Art. 5(2)). We propose a new subparagraph within Article 5(1) to read as follows:

> **(1)(j) Legibility of infrastructure**: Personal data shall be processed in a manner that enables the controller to demonstrate, with reasonable accuracy, the locations, routes, and technical environments through which such data is transmitted, including during transit, storage, and routing operations.

In this regulatory context, **legibility** refers to the capacity of a data controller to map, document, and disclose the technical paths, jurisdictions, and infrastructures through which personal data is transmitted, stored, and processed, such that regulatory authorities and data subjects can meaningfully evaluate compliance with the GDPR.

This principle of infrastructural legibility is intended to operate at the intersection of technical documentation and legal accountability. It imposes a minimum requirement on controllers to know and be able to disclose how data travels through their systems. Crucially, it does not mandate territorial retention or full localisation. It requires that if a controller routes personal data through a distributed system, it must retain sufficient operational knowledge to trace that movement and justify it under the GDPR's existing legal standards, especially those governing cross-border transfers under Chapter V.

This proposal is rooted in existing enforcement logic. Article 30 GDPR already requires controllers to maintain records of processing activities, including categories of data, purposes of processing, and recipients of data. The EDPB's Recommendations 01/2020 further require exporters to "know their transfers," including the countries to which data is sent and the legal basis for such transfers. However, neither of these provisions has been interpreted to include routing paths or infrastructural disclosure. As a result, controllers may remain GDPR-compliant on paper while being operationally blind to the most critical element of transborder data governance: where personal data is physically or virtually processed.

The need for reform is not academic. As established in Chapter 4, Starlink qualifies as a data controller under Article 4(7) and is therefore bound by all core provisions of the GDPR. Yet its infrastructure makes it functionally impossible to fulfil those obligations. Data transmitted by an EU user may be routed across orbital nodes and downlinked in third countries without any disclosure, logging, or external audit. Starlink's current privacy policies make no mention of routing decisions, ground station locations, or the criteria under which data is transmitted through non-EU jurisdictions. Nor does it publish any information about the use of safeguards such as standard contractual clauses or adequacy decisions.

This situation is not unique to Starlink. As discussed in Chapter 1 and the literature review, other LEO satellite providers such as OneWeb and Amazon Kuiper operate similar orbital architectures, with decentralised relays and mobile routing paths. The problem is therefore systemic: without infrastructural legibility, enforcement becomes structurally disabled. Supervisory authorities cannot verify whether Chapter V obligations are triggered, and users cannot determine whether their rights under Articles 13, 14, or 15 are being respected. The GDPR's accountability mechanism, outlined in Article 5(2), assumes that the controller has control over, or at minimum knowledge of, the processing environment. In satellite-based systems, this assumption is no longer valid.

Embedding infrastructural legibility in Article 5 would also align with broader EU regulatory trends. The NIS2 Directive, which governs cybersecurity in essential service providers, already mandates that such entities perform risk assessments, document system architecture, and notify authorities of operational changes. Likewise, the Digital Services Act (DSA) and the upcoming Cyber Resilience Act reflect a growing shift toward proactive documentation and transparency obligations in the management of digital infrastructure. A parallel requirement under the GDPR would therefore be both doctrinally coherent and institutionally feasible. It would not impose an unprecedented burden on controllers but would align the Regulation with the EU's broader regulatory ecosystem.

From a legal drafting perspective, the proposed amendment could be introduced through one of two routes. The first is formal treaty revision via the ordinary legislative procedure, whereby the European Commission proposes an amendment to the GDPR text, followed

by adoption through the Council and Parliament. This path, while legally robust, is politically challenging and may take years. The second option is to issue delegated legislation or an implementing act under Article 92 GDPR, authorising the Commission to provide further specification of the obligations under Article 5 in light of emerging technologies. Given the urgency of the problem and the demonstrated enforcement gap, the latter may be more realistic in the short term.

To support compliance, the reform could also be accompanied by an EDPB technical guidance document, modelled on Recommendations 01/2020, that specifies what counts as "reasonable accuracy" in the context of routing disclosure. For example, the guidance might state that where a provider relies on dynamically shifting routing paths (e.g. based on satellite availability), it must disclose: (1) the range of possible ground station locations; (2) the technical logic that governs routing decisions (e.g. latency optimisation); and (3) whether the system permits routing to third countries with inadequate protection under Article 45.

It is important to emphasise that this reform does not seek to impose an unrealistic burden on all data controllers. It is targeted at those operating decentralised or non-local infrastructures that pose a structural risk to enforcement. Traditional ISPs, cloud providers with regional zones, and on-premise data controllers would be largely unaffected. The purpose is not to increase bureaucracy but to close a specific regulatory loophole that allows orbital infrastructure operators to bypass scrutiny.

The Meta Ireland decision serves as a useful comparator. In that case, the controller was fined €1.2 billion for failing to implement sufficient safeguards when transferring data to the United States. The decision was grounded in Meta's inability to demonstrate that its SCCs provided "essentially equivalent" protection as required by Schrems II. In contrast, Starlink makes no such attempt. It does not offer any documentation of safeguards, nor does it even acknowledge the legal significance of its routing decisions. The proposed reform would make such exceptions legally untenable.

Moreover, by enshrining infrastructural legibility in Article 5, the GDPR would acquire a forward-looking adaptability that allows it to confront emerging technologies without constant revision. As observed in Chapter 2, the Regulation was drafted at a time when

terrestrial networks and cloud-based data centres dominated. But the digital landscape is changing. Connectivity is becoming more distributed, more automated, and less tied to physical jurisdiction. If the GDPR is to remain effective in this environment, it must evolve from a territorial model of enforcement to one grounded in infrastructural oversight.

Finally, the reform would carry important normative value. It would reaffirm the principle that data protection is not merely about consent or notice, but about the enforceable traceability of personal data across systems. It would restore to users the right not merely to be informed, but to understand and challenge the environment in which their data is processed. And it would send a clear message to infrastructure providers that operational opacity is not an excuse for regulatory evasion.

In conclusion, the proposed amendment to Article 5 addresses a specific and urgent problem in the Regulation's current architecture. By introducing a requirement of infrastructural legibility, the GDPR would regain its capacity to function in decentralised systems such as Starlink. This reform is not speculative. It is grounded in case law, consistent with broader regulatory practice, and operationally feasible through existing legal instruments. It reflects the central finding of this thesis: that data protection in space is not only a matter of jurisdiction, but of visibility. If the GDPR cannot see how data moves, it cannot protect it. The law must therefore adapt; not by abandoning its principles, but by making them enforceable in the infrastructures of the present.

6.2 Mandating Routing Transparency: A precondition for Enforcement

The preceding section established that the GDPR must be amended at the level of principle to address structural enforcement failures in decentralised data infrastructures, specifically in the context of satellite internet services. However, legal principles alone do not render the Regulation enforceable. Without operational instruments, even a reformed Article 5 remains inert. The GDPR's commitment to data protection by design and by default, to user rights, and to cross-border accountability is undermined not only

by technical complexity but by the absence of institutional leverage. Starlink and similar LEO-based services demonstrate that a controller's knowledge of data routing has become optional. This section argues that a practical, enforceable policy tool must be introduced to render data routing visible and legally actionable. It proposes a mandatory Routing Disclosure Statement (RDS) as a minimum transparency requirement for any satellite internet provider operating within the European Union and servicing EU-based data subjects. Such a tool is not theoretical. It is urgently necessary and already technically feasible. Its purpose is simple: to make routing visible, knowable, and assessable. Without it, all the obligations discussed in Chapters 3 through 5 collapse into a normative vacuum.

Routing transparency is the backbone of enforceable cross-border data governance. Without documentation of routing paths, no supervisory authority can determine whether a data transfer has occurred, and therefore whether Chapter V safeguards must be applied. This absence of transparency turns the Regulation's own logic into a circular trap: it cannot assess cross-border transfers unless it already knows a transfer has happened. This circularity, which providers such as Starlink exploit to avoid scrutiny, is not merely inconvenient, it is fatal to the GDPR's extraterritorial promise under Article 3(2). Starlink's routing architecture is governed by algorithmic logic optimised for network performance and latency. Nowhere in its public disclosures is there any mention of ground station locations, downlink jurisdictions, or the legal regimes governing its transmission pathways. If data is routed from an EU user via an orbital link and downlinked in a non-adequate third country, and no safeguard or user information is applied, this may constitute a violation of Article 44. But in the absence of transparency, neither the user nor the supervisory authority can verify this. Transparency is not a luxury but a mechanism through which accountability can operate in distributed infrastructure.

The proposed policy instrument is the Routing Disclosure Statement. It is a structured, auditable document submitted annually by all providers of non-terrestrial connectivity whose infrastructure is technically capable of cross-border routing. The obligation to submit this document would apply regardless of whether the provider believes such routing constitutes a transfer. The very purpose of the Statement is to allow that determination to be made transparently. In practice, the RDS would be similar in function

to the risk documentation required under Article 35 GDPR (Data Protection Impact Assessments) or the records of processing activities required under Article 30. It would serve as an infrastructural supplement to those records: a demonstration not only of processing purpose and category, but of physical and jurisdictional routing paths. The submission would include: (a) a list of all ground stations used or available for data downlink from EU-based users; (b) the jurisdictions in which those stations are located and the legal basis under which those jurisdictions are assessed (adequacy, SCCs, Article 49 derogations); (c) a summary of routing logic, including how routing decisions are made in real time, what parameters govern satellite-to-ground and satellite-to-satellite switching, and whether legal considerations play any role in such decisions; (d) a declaration of potential third-country exposure; and (e) the internal governance structures responsible for monitoring routing transparency and compliance with Article 44 and 46.

The purpose of this Statement is not to demand real-time data, nor to require exhaustive network logs. Rather, it is to establish an enforceable baseline of knowledge, or in other words: a minimal visibility requirement. Without such a baseline, the GDPR cannot be enforced against actors whose infrastructures are designed to bypass territorial jurisdiction. Starlink's vertically integrated control of both its satellites and ground infrastructure makes such disclosure not only possible but already available internally. What is missing is the legal obligation to externalise that knowledge and subject it to regulatory assessment.

This proposal aligns with broader EU regulatory developments that embed transparency into the governance of critical infrastructure. Under the NIS2 Directive, providers of essential services must document their systems, submit incident reports, and provide architectural maps to national cybersecurity authorities. Similarly, the Digital Operational Resilience Act (DORA) requires financial entities to map their ICT dependencies, conduct risk assessments, and notify regulators of critical changes. These frameworks accept a simple premise: that modern governance of decentralised, digital infrastructure cannot function without structural visibility. The GDPR, although normatively ambitious, has yet to adopt this operational realism. The RDS fills that gap. It ensures that when personal data is transmitted through systems whose technical operations may override legal safeguards, there is at least an auditable record of that movement. The EDPB

Recommendations 01/2020 are already clear: controllers must "know their transfers." The RDS transforms that guidance into a compliance requirement.

Legally, the obligation could be introduced through a delegated act by the European Commission under Article 92 GDPR, which allows the Commission to adopt measures for the uniform application of the Regulation. Alternatively, the EDPB could issue formal guidance under Article 70(1)(e), accompanied by a standardised template and technical annex, setting out what constitutes a compliant RDS. Ideally, both instruments would operate in tandem: delegated legislation to establish the legal requirement, and EDPB guidance to provide implementation detail. This dual mechanism would ensure both enforceability and interpretive coherence across Member States.

Enforcement of the obligation would fall to national DPAs, supported by ENISA for technical evaluation. The EDPB could host a centralised RDS portal, where Statements are logged, publicly summarised, and available for audit. In cases of non-compliance (such as failure to submit, submission of manifestly incomplete information, or disclosure revealing non-compliant routing) DPAs could initiate corrective measures under Article 58, impose administrative fines under Article 83, or suspend transfers under Article 66. To incentivise compliance, the RDS could be integrated into certification schemes under Article 42 or used as a prerequisite for EU digital infrastructure tenders. In the medium term, routing transparency could become a standard procurement clause for public digital services, particularly where citizen data is involved.

It is anticipated that providers may object on grounds of confidentiality or feasibility. These objections are unfounded. The RDS does not require disclosure of proprietary algorithms, only the outcomes those algorithms produce. It does not require live tracking, only annual or incident-based summaries. It does not expose trade secrets but documents jurisdictional exposure. The analogy with financial risk reporting is instructive: institutions disclose operational exposure not to reveal internal strategies, but to allow regulators to assess systemic vulnerabilities. The same logic applies here. Providers who refuse to disclose routing architecture effectively claim the right to process personal data without oversight. This is incompatible with both the spirit and structure of the GDPR.

Moreover, the RDS is designed not to constrain innovation, but to ensure that innovation does not create zones of legal non-enforcement. The existing situation creates a dangerous incentive: the unclearer and more decentralised a provider's infrastructure becomes, the less enforceable the law becomes. This undermines regulatory legitimacy and rewards evasive architecture. A disclosure obligation reverses that logic. It creates a compliance floor, without which no controller can lawfully process data across borders. In doing so, it re-establishes the link between legal jurisdiction and technical operation.

The proposal also advances user rights. Articles 13 and 14 require that data subjects be informed of where and how their data is processed. Article 15 gives them the right to access that information. Currently, these rights are empty when applied to LEO satellite services. Starlink does not disclose routing practices to users. Nor does it inform them of potential third-country downlinks. The RDS would enable DPAs to demand public summaries of routing logic and would allow users to make informed decisions about the legal exposure of their personal data. It would also enable the exercise of the right to object (Article 21), particularly where routing into certain jurisdictions creates disproportionate risks.

Finally, the requirement would support future legal development. As noted in Chapter 2.3, the GDPR was not drafted for a world in which data no longer touches the jurisdiction whose laws are supposed to govern it. The rise of orbital systems, mesh networking, and edge computing threatens to displace law as the primary framework of data governance. The RDS is therefore not merely a transparency tool. It is a jurisdictional anchor. It signals that Europe will not accept a model of digital infrastructure in which legal oversight becomes structurally impossible. By forcing the documentation of routing decisions, the EU asserts that legal compliance must remain a condition for market access.

In sum, the Routing Disclosure Statement is the practical hinge that connects legal principle to technical enforcement. Without it, Article 5's reform is declaratory. With it, the GDPR regains control over infrastructures designed to bypass jurisdiction. The Statement imposes no new principle but renders existing principles enforceable. It demands no territorial redesign, only transparency. It does not police innovation but sets the minimum conditions under which innovation may operate in lawful space. In a world

where routing is algorithmic and borderless, visibility is power. The RDS gives that power back to the law.

6.3. Data Embassies as a Jurisdictional Fallback in Infrastructure Enforcement

The two preceding sections have offered doctrinal and operational solutions to the enforcement void identified throughout this thesis. By proposing an amendment to Article 5 and a binding routing disclosure mandate, the previous sections advanced regulatory tools that render satellite internet infrastructures visible, traceable, and therefore subject to European data protection law. Yet even these measures may encounter residual enforcement obstacles in practice. Where third-country providers resist routing transparency, or where extraterritorial infrastructure renders both territorial jurisdiction and cross-border safeguards difficult to enforce, the European Union must consider auxiliary instruments of legal containment. This section proposes a complementary, though necessarily limited, mechanism: the adoption of data embassies as sovereign extensions of EU legal jurisdiction. These embassies are not replacements for data protection enforcement mechanisms, nor are they suitable as a primary regulatory tool. Rather, they are a conditional safeguard designed to preserve GDPR applicability in infrastructural contexts where neither localisation nor oversight can otherwise be guaranteed.

The concept of the data embassy is not hypothetical. Its most prominent implementation has occurred in Estonia, which, following a large-scale cyberattack in 2007 and subsequent concerns over national resilience, negotiated a bilateral agreement with Luxembourg to house copies of critical Estonian governmental databases in a facility located on Luxembourgish territory. The crux of this agreement is that the data centre, while geographically outside Estonia, is subject exclusively to Estonian jurisdiction. The legal arrangement is based on a modified reading of the Vienna Convention on Diplomatic Relations (VCDR), specifically Articles 22 and 24, which establish the inviolability of diplomatic premises and archives. While the VCDR was designed to

protect physical embassies and communications, the Estonian model creatively extends its logic to digital assets. In effect, the data embassy transforms foreign-located servers into sovereign legal enclaves, governed by the laws of the home country and immune from the jurisdiction of the host state.

This model offers an attractive workaround to the jurisdictional dislocations inherent in orbital infrastructure. As shown in Chapter 4, the GDPR's territorial scope under Article 3(2) is frustrated not by doctrinal uncertainty but by infrastructural opacity. Starlink does not localise its routing, does not provide access to routing logs, and does not offer any transparency as to the jurisdictions in which user data is downlinked. Even if Article 5 is amended and routing disclosure is mandated, enforcement remains vulnerable to refusals by third-country actors or to geotechnical constraints that make compliance difficult. In such cases, the data embassy presents an option of last resort: a bilateral agreement by which data processed in or through third-country territory is housed in a server environment that remains legally bound by European data protection law and verifiably insulated from the jurisdictional reach of the host country.

Such a model could apply not only to storage but also to operational downlinks or interconnection points. For instance, if a Member State partners with a satellite provider whose infrastructure requires ground stations in non-adequate third countries, a data embassy agreement could be used to designate those stations, or a segment thereof, as sovereign-controlled spaces subject exclusively to EU law. The same principle could apply to data centres handling telemetry or payload data derived from European users. What matters is not the absolute localisation of infrastructure but the preservation of legal sovereignty over personal data within that infrastructure.

This approach would be legally feasible under the GDPR. Article 46(3)(a) allows for the use of "contractual clauses or provisions" authorised by a competent supervisory authority and approved by the Commission as valid grounds for cross-border transfers in the absence of an adequacy decision. A data embassy agreement, codified as a treaty between an EU Member State and a third country, could serve as such a provision, provided it includes enforceable safeguards, audit rights, and jurisdictional exclusivity clauses. In this sense, the data embassy would function as a bespoke transfer mechanism,

akin to Binding Corporate Rules or tailored SCCs, but grounded in international law rather than private contracts.

To operationalise this model within the GDPR framework, the European Commission could develop a model agreement, similar in function to the standard contractual clauses currently used under Article 46(2)(c). This model would set minimum standards for data embassy agreements, including: (a) legal immunity from host country access or jurisdiction; (b) enforceable dispute resolution mechanisms under EU law; (c) mandatory technical and organisational safeguards equivalent to those required under Article 32 GDPR; and (d) audit rights for the home state's supervisory authority. Such a model could then be adopted by Member States seeking to negotiate embassy-based hosting arrangements for critical or sensitive data. This would both reduce fragmentation and provide a harmonised baseline for evaluating whether such embassies meet the requirements of Article 46.

Nevertheless, while the model is normatively appealing and legally grounded, it is not without limitations. The most significant of these is its bilateral nature. Data embassy agreements, by definition, require diplomatic negotiation, treaty ratification, and infrastructure planning. They are resource-intensive, slow to conclude, and dependent on the cooperation of third-country governments. In an increasingly fragmented geopolitical environment, it may not always be feasible to secure such agreements - particularly with countries whose legal systems or strategic interests diverge from those of the European Union. Moreover, the application of the VCDR to data centres, while conceptually innovative, remains legally untested at scale. Although Estonia's model has not been challenged, its generalisability is uncertain. Were the concept to be applied in a high-stakes commercial or geopolitical context, questions might arise about the enforceability of jurisdictional immunity and the legal basis for treating digital infrastructure as inviolable diplomatic premises.

A further limitation lies in the model's applicability to real-time routing and dynamic transmission. While a data embassy may secure storage or processing environments, it cannot substitute for live routing transparency. In the context of satellite internet, where data is transmitted across orbital links and downlinked according to latency-optimised

algorithms, the embassy model provides no mechanism for observing or controlling those decisions. It may secure the endpoint, but it cannot oversee the path. Thus, it cannot address the metadata-level concerns raised in Chapter 5, nor can it resolve the accountability gap created when routing paths are determined by non-legal parameters. In this sense, the data embassy should be seen not as a routing safeguard but as a jurisdictional fallback: a means of securing data post-processing, not during transmission.

There are also institutional challenges. If each Member State negotiates its own data embassy agreements, there is a risk of legal fragmentation, conflicting standards, and forum shopping. Providers may seek to partner with Member States offering weaker enforcement or looser definitions of sovereignty. To mitigate this risk, the Commission must play a central role in coordinating and standardising data embassy arrangements. This coordination could take the form of a Directive establishing conditions for Member State negotiations, or a delegated act setting out binding criteria for the recognition of such embassies under Article 46 GDPR. Alternatively, the EDPB could issue guidance establishing that only treaties conforming to its model agreement qualify as valid safeguards.

Despite these limitations, the data embassy model offers a viable solution in specific, high-risk contexts. It is particularly suited to strategic public-sector data, high-sensitivity datasets, or core connectivity infrastructure operated by non-EU providers. For example, should an EU Member State contract a foreign satellite provider for national defence communications, but be unable to secure full routing transparency or localisation, a data embassy agreement could preserve sovereignty over the resulting data flows. The same applies to meteorological, environmental, or disaster response data, where the public interest in lawful processing is particularly acute.

In these cases, the data embassy ensures that even where the infrastructure cannot be physically brought within the Union, the law can be. This inversion of the localisation paradigm (bringing the law to the data, rather than the data to the law) is both consistent with the GDPR's underlying objectives and responsive to the technological shifts discussed throughout this thesis. The embassy model does not displace the need for

routing transparency or infrastructure reform. It supplements them. It is a residual mechanism for legal containment when more direct forms of oversight fail.

In conclusion, this section has proposed the data embassy as a jurisdictional fallback mechanism within the GDPR's regulatory architecture. Based on established diplomatic principles and implemented in practice by Estonia, the model offers a treaty-based solution to cross-border enforcement in satellite and decentralised infrastructures. While limited by its bilateralism and its inability to monitor live routing decisions, it provides a practical safeguard where legal control over physical infrastructure is not possible. Its adoption should be encouraged only in targeted cases, supported by a harmonised EU framework, and clearly distinguished from general transfer mechanisms. In an era where infrastructure transcends borders, sovereignty must be redefined not as a function of geography, but of legal enforceability. The data embassy offers one path toward that redefinition: one that complements, rather than replaces, the regulatory strategies advanced in the preceding sections.

Chapter 7: Conclusions

7.1 Findings

This thesis has explored whether the General Data Protection Regulation (GDPR), as currently designed, can provide effective protection for personal data processed through decentralised, satellite-based internet infrastructures. The analysis has been structured around the case study of Starlink, a network operated by SpaceX that delivers internet connectivity through a constellation of low Earth orbit (LEO) satellites. Starlink has been chosen not as an anomaly but as a representative of a broader shift in how digital infrastructure is deployed and operated. The findings of the thesis, while grounded in this case, extend far beyond any single provider. They illuminate a systemic challenge that touches upon the doctrinal coherence, enforceability, and regulatory resilience of European data protection law in the context of emerging, extraterritorial technologies.

The central finding is unequivocal: while the GDPR applies to services such as Starlink in principle, its enforcement architecture is rendered structurally ineffective in practice. This ineffectiveness arises not from a lack of legal authority, but from a mismatch between the legal system's assumptions and the technical characteristics of modern orbital infrastructure. Starlink's routing architecture, which relies on dynamic satellite relays and shifting ground station linkages, severs the connection between data processing and physical geography upon which the GDPR depends. The result is a regulatory environment where neither users, data controllers, nor supervisory authorities can ascertain where personal data is processed, whether it is transferred to third countries, or what legal safeguards apply.

The thesis began in Chapter 1 by outlining the research problem: that satellite-based internet services undermine the spatial assumptions embedded in the GDPR. Traditional internet service providers (ISPs) operate through fixed terrestrial infrastructure that can be mapped, inspected, and regulated. By contrast, Starlink routes data via satellites that orbit the Earth continuously and use inter-satellite laser links to relay data between nodes. These routes are determined by factors such as latency optimisation and bandwidth availability, rather than legal or jurisdictional boundaries. Ground stations that downlink data may be located in third countries, and their selection is driven by network efficiency

rather than compliance logic. This architecture creates a situation in which data routing is opaque even to the controller, let alone to users or regulators. The introduction framed this problem not only as a matter of legal uncertainty but as a broader structural challenge to the enforceability of data protection rights.

Chapter 2 reviewed the literature on cross-border data flows, the territorial scope of the GDPR, and prior discussions of jurisdictional fragmentation. The analysis found that while scholars such as Kuner, Voss, and de Hert have extensively discussed the conceptual and doctrinal challenges of global data governance, their work largely assumes infrastructure that is still terrestrial, cloud-based, or at least geographically legible. What is absent from the literature is a sustained engagement with infrastructure that is non-territorial by design. The literature acknowledges the ambiguity surrounding the definition of a data transfer and the limitations of extraterritorial enforcement but often presumes that data routes can be known, logged, and assessed. This thesis identified a significant research gap at the intersection of infrastructure design and legal enforceability. It argued that LEO satellite systems, such as those used by Starlink, introduce a new form of opacity that is not simply the product of complexity but is structurally incompatible with the GDPR's foundational principles.

Chapter 3 developed a detailed comparison between traditional ISPs and Starlink. It highlighted how terrestrial ISPs are subject to domestic legal regimes, including sector-specific laws such as the ePrivacy Directive. These ISPs operate within national jurisdictions, are registered with data protection authorities, and can be audited or sanctioned if they breach data protection law. Their data routing paths, while sometimes complex, are generally traceable, and their compliance structures are embedded within national oversight mechanisms. In contrast, Starlink's infrastructure is decentralised, mobile, and largely inaccessible to regulators. The company does not disclose which satellites or ground stations are used for specific transmissions, and it does not offer any commitment that data originating from European users will remain within the European legal space. The chapter argued that this disjunction renders comparisons between Starlink and traditional ISPs fundamentally misleading. While both deliver internet access, the architecture through which they operate presents entirely different conditions for legal oversight and user accountability.

Chapter 4 applied the GDPR directly to Starlink's model. It analysed the Regulation's scope under Article 3, the classification of Starlink as a data controller under Article 4, and the requirements concerning data processing, user rights, and international transfers under Articles 5, 13 to 22, 32, and 44 to 49. The findings demonstrated that while Starlink clearly falls within the GDPR's territorial scope by virtue of targeting EU data subjects, its infrastructure undermines the very mechanisms by which compliance can be assessed. The company does not publish any privacy notice specific to routing decisions, does not disclose the location of ground stations, and does not inform users about the potential for third-country transfers. Without this information, the obligations imposed by the GDPR on transparency, accountability, and lawful transfer cannot be fulfilled. The chapter further examined case law such as Schrems II and Tele2 Sverige, showing that the Court of Justice of the European Union has repeatedly affirmed that enforceable rights must accompany data wherever it is processed. Starlink's model breaks this logic. If neither the user nor the controller can identify where data is processed, then legal obligations under Chapter V are rendered practically meaningless.

Chapter 5 of this thesis assessed the implications of this legal breakdown from three perspectives: jurisdictional loss, regulatory arbitrage, and the erosion of user rights. It found that the GDPR's enforcement architecture depends on infrastructural traceability. If data flows cannot be mapped, then supervisory authorities cannot verify whether safeguards have been applied, whether transfers are lawful, or whether users have been informed. Starlink's design creates a condition of enforced ignorance, not because of negligence, but because the architecture itself severs the link between data movement and legal visibility. This was defined as a form of regulatory arbitrage, not in the traditional sense of forum shopping, but in the structural sense of placing data beyond the reach of any one jurisdiction by default. The GDPR cannot be enforced where no jurisdiction can claim visibility over the processing event. This conclusion was not limited to regulators. The chapter also demonstrated that users are systematically denied their rights. Without routing transparency, users cannot invoke their rights of access, rectification, objection, or portability, because they do not know who holds their data, where it is stored, or under what legal conditions. The GDPR promises these rights in theory, but they fail in systems like Starlink where infrastructural opacity is a design feature.

In Chapters 6 the thesis advanced a three-part policy solution designed to respond directly to the structural failings identified in the earlier analysis. First, it proposed the amendment of Article 5 to introduce a principle of infrastructural legibility. The new provision would require that data controllers be able to demonstrate, with reasonable accuracy, the locations, routes, and technical environments through which personal data is processed. This proposal is grounded in existing legal duties under Articles 30 and 32, as well as in the EDPB's recommendations on mapping data transfers. The amendment would not impose localisation but would require that controllers retain operational knowledge of their own infrastructure. Without such knowledge, legal obligations under the GDPR become hollow.

Second, the thesis proposed the creation of a mandatory Routing Disclosure Statement (RDS) for all providers of non-terrestrial internet connectivity operating in the European market. This instrument would require providers to declare the locations of their ground stations, the logic governing routing decisions, and the legal mechanisms used to safeguard cross-border data flows. This proposal addresses the operational gap identified in Chapters 4 and 5: that even if obligations exist, they cannot be assessed without technical disclosure. The RDS would render the GDPR's transfer rules enforceable by creating a factual basis upon which regulators could intervene. It also aligns with broader EU digital governance trends, such as those found in the NIS2 Directive and the Digital Operational Resilience Act, which require documentation and oversight of critical infrastructure.

Third, the thesis explored the concept of data embassies as a jurisdictional fallback. Building on the Estonian model, it argued that Member States could negotiate bilateral treaties that establish extraterritorial data centres under exclusive European jurisdiction. While not a substitute for routing transparency, data embassies could offer a legal enclosure for data that cannot be localised but must be protected. The use of such agreements, recognised under Article 46(3) GDPR, would preserve the applicability of European law to critical datasets and provide an institutional mechanism for controlling access, enforcing safeguards, and conducting audits. However, the thesis acknowledged that this approach is limited by its bilateral nature and may not be scalable across the

entire digital economy. It is best understood as a supplementary tool for high-risk or strategic data, rather than a general solution.

Taken together, the findings of this thesis point to a clear conclusion: the GDPR, while normatively robust, lacks the operational instruments necessary to regulate infrastructures that fall outside territorial logic. Starlink is not a lawless entity, but it operates in an infrastructural context where law cannot see, cannot verify, and therefore cannot protect. This mismatch is not an anomaly; it is a structural consequence of how internet delivery is changing. As more services shift to orbital, distributed, or edge-based architectures, the problem identified in this thesis will only become more pressing. Legal reform is therefore not a matter of closing loopholes, but of retooling the very assumptions upon which regulatory power depends.

The policy proposals developed in Chapter 6 respond directly to these doctrinal failures. The need for infrastructural legibility builds upon longstanding concerns about the definitional ambiguity of 'transfer' (Kuner 2011), the enforcement vacuum created by extra-territorial infrastructures (Voss 2020), and the weakening of jurisdictional anchors in digital environments (de Hert and Czerniawski 2013; Koops and Goodwin 2019). These interventions are not speculative. They are grounded in a body of scholarship that has long cautioned against assuming that legal protections will remain enforceable as infrastructure evolves. The solutions proposed here offer a targeted and institutionally realistic path forward: one that restores the preconditions for regulatory oversight without undermining the core principles of the GDPR. If Europe is to uphold its normative leadership in data protection, it must ensure that its legal framework adapts to the infrastructures through which data now flows.

This summary of findings has demonstrated that the current enforcement model of the GDPR cannot withstand the pressures introduced by decentralised and opaque routing systems. While the Regulation remains formally applicable, its capacity to deliver on its core promises, that is transparency, accountability, and enforceability, is compromised by the infrastructures through which data is now transmitted. The policy solutions proposed in this thesis aim to restore that capacity, not by altering the fundamental principles of the GDPR, but by extending its reach into the technical systems that now mediate digital life. The final section of this thesis will reflect on the broader implications of these findings

and outline how European data protection law must evolve if it is to remain effective in the age of orbital communications.

7.2 Answering the Research Questions

This thesis began with one central question:

Can the GDPR, in its current form, provide effective protection for personal data processed through space-based internet services such as Starlink?

The answer, based on the findings of the preceding chapters, is no. While the Regulation formally applies to providers such as Starlink through its extraterritorial scope under Article 3(2), the infrastructure on which these services rely renders its application functionally unenforceable. The GDPR assumes a degree of spatial and technical visibility that Starlink's architecture, by design, does not permit. Without infrastructural legibility, the Regulation's core principles become ineffective in practice.

This conclusion is supported throughout the thesis by a detailed examination of both technical and legal conditions. As Chapter 3 demonstrated, Starlink's routing model bypasses traditional territorial infrastructure by using inter-satellite laser links and non-EU ground stations selected on the basis of latency, not jurisdiction. These operational characteristics sever the link between data movement and legal oversight. In Chapter 4, the legal obligations imposed by Articles 13, 14, 15, 44, and 46 were shown to be unfulfillable when the controller cannot determine or disclose where data is processed. The inability to map data flows undermines the user's right to access, the controller's duty to inform, and the regulator's capacity to audit or intervene.

These findings give rise to the following answers to the four sub-questions introduced in Chapter 1.2.

1. How does Starlink's technical infrastructure differ from that of traditional ISPs, and what implications does this have for jurisdiction and legal oversight?

Starlink's infrastructure departs from the fixed, terrestrial model of traditional ISPs by routing data via a decentralised mesh of satellites. Unlike national ISPs, which operate within traceable and auditable fibre-optic networks, Starlink transmits data through dynamically shifting orbital pathways and foreign ground stations. As shown in Chapter 3, this makes it impossible to identify processing locations with consistency or to assign jurisdictional responsibility with confidence. The regulatory tools designed for terrestrial ISPs, such as data localisation, contractual safeguards, and infrastructure-based audits, fail to operate effectively when applied to a non-territorial architecture. Consequently, the GDPR's mechanisms for ensuring compliance, redress, and user control lose their practical relevance.

2. To what extent can data routing through non-EU satellites or ground stations be considered a cross-border transfer under the GDPR?

The thesis has shown that Starlink's infrastructure likely triggers international data transfer rules under Chapter V of the GDPR. When EU user data is routed through orbital relays and downlinked in third countries, a transfer in the legal sense has probably occurred. However, as Kuner notes, "it is difficult to apply the concept of transfer to situations where data is mirrored or backed up across multiple jurisdictions simultaneously" (Kuner 2011, 32). This ambiguity is intensified in Starlink's case because the system does not disclose routing paths and does not allow either the controller or the user to identify when and where a transfer has taken place. The legal obligation to apply safeguards under Article 44 is rendered unenforceable, not because the provision is flawed in substance, but because the infrastructural opacity makes it inapplicable in practice.

3. Does the current regulatory framework allow users and data protection authorities to verify how and where data is processed in satellite-based networks?

The findings indicate that verification is structurally impossible under current conditions. Starlink does not publish information on the ground stations it uses, nor does it provide

EU-specific assurances about routing practices. This violates the obligation of transparency under Articles 13 and 14 and prevents users from exercising their rights under Article 15. Regulatory authorities are likewise unable to conduct audits or enforce obligations, since the routing infrastructure is located outside their jurisdiction and is dynamically reconfigured in ways that resist mapping. As the FRA notes, "Data Protection Authorities across Member States often lack the resources, expertise, and cross-border mechanisms to engage with non-territorial infrastructure providers" (FRA 2024). Without a minimum degree of infrastructural visibility, the GDPR cannot be enforced, and user rights remain theoretical.

4. What regulatory measures could improve transparency, legal accountability, and enforcement in the context of non-territorial internet infrastructure?

The policy proposals advanced in Chapter 6 provide a structured response to this question. First, the thesis calls for an amendment to Article 5 GDPR that introduces a requirement of infrastructural legibility. This principle would require controllers to demonstrate knowledge of the locations, routes, and environments through which personal data is processed. Second, the thesis proposes a Routing Disclosure Statement (RDS), a binding transparency instrument through which providers of non-terrestrial connectivity would be required to disclose ground station locations, routing logic, and legal safeguards. Third, the thesis explores the use of data embassies as a jurisdictional fallback in contexts where full infrastructure control is infeasible. These proposals are not speculative. They emerge directly from the doctrinal challenges identified in Chapters 3 through 5 and are consistent with the GDPR's foundational objective: to ensure that personal data is subject to effective and enforceable protection, regardless of where or how it is processed.

The answers to these questions reveal that the central problem is not the unwillingness of controllers to comply, nor the inattention of regulators, but rather the design of the infrastructure itself. When legal systems cannot observe, locate, or verify the conditions under which personal data is processed, they lose their capacity to govern. The GDPR was crafted as a rights-based, technologically neutral regulation, but its enforcement architecture remains tied to assumptions of geographical anchoring and visible control.

As Koops and Goodwin write, “It is important to speak of a loss of knowledge of location rather than a loss of location” (Koops and Goodwin 2019, 9). Infrastructures like Starlink do not eliminate geography; they make it unknowable. This thesis has shown that such unknowability is not a technical inconvenience. It is a legal rupture.

In conclusion, the thesis has fulfilled its research aims by providing a detailed legal analysis of the GDPR’s current limitations, evaluating a representative case study in depth, and proposing legally and institutionally grounded reforms. The findings make clear that the GDPR is not outdated in its principles, but it is unequipped for a regulatory environment in which infrastructures are designed to obscure rather than expose the conditions of data processing. The proposals offered in this work aim to restore that exposure. They are not an expansion of legal scope, but a reassertion of legal enforceability in a context where opacity is fast becoming the norm.

7.3 Final Reflections

A new form of digital sovereignty is emerging, and infrastructure has become a site of political and legal contestation. As Ruggiu writes, “The economic space necessarily enters into tension with the normative space, continually generating non-places: juridically unregulated spaces or spaces that can be appropriated by another legal order” (Ruggiu 2022, 9). These non-places are not theoretical artefacts. Satellite internet infrastructures that bypass jurisdictional anchoring reshape the legal landscape itself, producing environments in which legal norms cannot be enforced and political accountability is displaced. In this context, the problem examined in this thesis becomes more than a matter of regulatory nuance. It becomes a question of legal capacity: whether the European legal order, and the GDPR in particular, can retain authority over infrastructures that are extraterritorial, privately controlled, and increasingly opaque. Satellite internet services such as Starlink are not neutral technologies. They are geopolitical instruments with direct implications for national security, communications sovereignty, and the enforceability of European rights. As the Italian parliamentary debate of February 2025 made clear, the presence of non-European infrastructure in

sensitive sectors is no longer being viewed with legal indifference. It is becoming a matter of strategic concern.

That said, this thesis does not pretend to have answered all questions, nor to have resolved all regulatory uncertainties. There are clear limitations in scope and methodology that must be acknowledged. This research is doctrinal and conceptual. It does not include empirical access to Starlink's internal routing data, nor does it provide a forensic technical audit of satellite transmissions. It has relied on secondary sources and publicly available infrastructure documentation, which means that some of the architectural claims remain necessarily general. The thesis has also not addressed the full spectrum of international law or space law provisions that might intersect with data protection norms in outer space. These areas deserve deeper investigation.

Moreover, the policy proposals advanced here are deliberately targeted but will require further refinement and testing before they can be implemented. The concept of infrastructural legibility, while intuitively powerful, needs to be explored further in comparative regulatory contexts. Similarly, the feasibility and legal status of data embassies beyond the Estonian model must be developed through additional treaty law analysis and case studies. The Routing Disclosure Statement, as proposed, offers a baseline for transparency, but future work should explore how such a requirement could be reconciled with proprietary and security concerns, especially in dual-use infrastructures with military and civilian applications.

What this thesis does show, however, is that data protection law, and digital regulation more broadly, is no longer simply a technical field. It is a critical component of geopolitical strategy, institutional legitimacy, and democratic resilience. When legal frameworks fail to adapt to new infrastructures, the cost is not merely theoretical. It is borne by individuals who lose access to enforceable rights, by regulators who are unable to intervene, and by states that lose the ability to uphold their legal values in the face of extraterritorial technologies. The GDPR is often praised for its ambition, but its credibility will ultimately depend on its capacity to govern the infrastructures of the future, not just those of the past.

In this light, the topic explored here is not only relevant but urgent. The law of digital innovation must now confront the fact that innovation has outpaced jurisdiction. As connectivity moves beyond borders, the law must follow, not through assertion alone, but through mechanisms that render rights enforceable in the systems that matter most. This thesis has aimed to make a contribution to that effort, by showing how legal obligations collapse when infrastructure becomes opaque, and by proposing practical ways to restore transparency and accountability without abandoning the principles on which the GDPR is built.

Further research is needed. This topic should not be treated as a niche problem affecting a marginal class of providers. It is an early signal of a much broader transformation in how legal systems interact with code, infrastructure, and global technical networks. The law of the future will not only regulate platforms and content. It will need to grapple with satellites, cables, protocols, and hardware. Legal scholars, technologists, and policymakers will need to work together more than ever before. The regulatory problems of the coming decade will not be resolved within disciplinary silos. They will require interdisciplinary fluency, geopolitical awareness, and the courage to update legal systems without compromising their normative commitments.

In this spirit, the work presented here should be read not as a definitive solution, but as an opening contribution to a legal field in transition. If it has clarified how jurisdiction collapses in the face of invisible infrastructure, and if it has offered at least one set of tools to begin addressing that collapse, then it has served its purpose. The question now is whether legal and institutional actors will act on these findings or whether the protection of personal data will become another casualty of architectures we can no longer see.

Chapter 8: References

Catanzariti, M. (2022). Disconnecting Sovereignty: Infrastructures, Data, and Law. Springer.

Catanzariti, M. (2022). Lo spazio dei dati. Nuove tensioni tra diritto, sovranità e infrastrutture. Ars Interpretandi, 2, 7–103.

Court of Justice of the European Union. (2016). Judgment in Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson.

Court of Justice of the European Union. (2020). Judgment in Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II).

de Hert, P., & Czerniawski, M. (2013). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, 6(3), 230–243.

European Data Protection Board (EDPB). (2018). Guidelines 03/2018 on the territorial scope of the GDPR (Article 3). https://edpb.europa.eu

European Data Protection Board (EDPB). (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. https://edpb.europa.eu

European Data Protection Board (EDPB). (2021). Recommendations 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. https://edpb.europa.eu

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

European Union Agency for Cybersecurity (ENISA). (2024). Mapping the regulatory framework of cybersecurity and data protection in satellite communications. https://www.enisa.europa.eu

European Union Agency for Fundamental Rights (FRA). (2024). Fundamental Rights Report 2024. https://fra.europa.eu

Figg, R., et al. (2019). The Application of Data Protection Laws in (Outer) Space. Rothwell Figg White Paper. https://www.rothwellfigg.com

Koops, B.-J., & Goodwin, M. (2013). Cyberspace, the cloud, and cross-border criminal investigation. Michigan Journal of International Law, 41, 101–141.

Kuner, C. (2011). The regulation of transborder data flows under data protection and privacy law: Past, present and future. OECD Digital Economy Papers, (187). https://doi.org/10.1787/5kg0s2fk315f-en

Kuner, C. (2020). Data transfers and their discontents: Territoriality and the protection of personal data. European Data Protection Law Review, 6(1), 28–36.

Nkansah, L. A. (2016). Interdisciplinary legal research methodology: Challenges and prospects. Journal of Law, Policy and Globalization, 49, 1–28.

Pelton, J. N. (1998). Telecommunications for the 21st century. Scientific American, 279(3), 80–85.

Schrama, W. (2011). Interdisciplinary legal research: Method and challenges. Law and Method, 1, 145–167.

Siems, M. M. (2009). The taxonomy of interdisciplinary legal research: Finding the way out of the desert. Journal of Commonwealth Law and Legal Education, 7(1), 5–17.

Svantesson, D. J. B. (2016). Solving the Internet Jurisdiction Puzzle. Oxford University Press.

Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. Washington International Law Journal, 29(3), 485–525.

Yu, L. (2023). The GDPR and China: Extraterritorial Application, Cross-Border Data Transfers and Regulatory Interaction (Doctoral dissertation, University of Göttingen).