Lisbon School of Economics & Management
Universidade de Lisboa

MASTER

IN INNOVATION AND RESEARCH FOR SUSTAINABILITY

DATA GOVERNANCE AND GENERAL DATA PROTECTION REGULATION (GDPR) AS A COMPETITIVE ADVANTAGE FOR PROPULSE

Luis Jesus Maravi Sanchez

Supervision:

Anibal Lopez

ISEG. Lisbon, Portugal, May 2026

DATA GOVERNANCE AND GDPR AS A COMPETITIVE ADVANTAGE FOR PROPULSE

By Luis Jesus Maravi Sanchez

This thesis analyzes how Propulse, a technology startup, can turn GDPR compliance into a sustainable competitive advantage in the European market. Through a qualitative case study integrating data governance, *privacy by design*, DPIA, and algorithmic ethics, an operational model is built. Research incorporates expert interviews, startup benchmarking, and a practical pilot with Portuguese company Litehaus. Results indicate that rigorous data protection implementation enhances strategic indicators such as conversion rates, sales cycle duration, and reputational perception among European clients, while strengthening organizational resilience and enabling access to funding and tendering opportunities in sensitive sectors.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

In today's data intensive digital economy, the responsible management of personal information has become a strategic axis for companies of all sizes, especially those operating in technological and highly regulated sectors. The entry into force of the General Data Protection Regulation (GDPR) in 2018 marked a global milestone by establishing one of the most rigorous and demanding regulatory frameworks in terms of privacy, reshaping not only the legal obligations of organizations but also their institutional architecture, operational models, and legitimacy before clients, partners, and investors (Voigt & von dem Bussche, 2017; EDPLR, 2020).

The GDPR has transformed privacy from a mere technical requirement into a strategic dimension of differentiation. According to Gellert (2018) and Ryngaert (2020), those companies that integrate robust governance models from early stages, including principles such as *privacy by design*, impact assessments (DPIA), traceability, and interoperability controls, not only reduce their exposure to legal risks but also gain legitimacy in the market. This is especially true in sectors such as proptech, fintech, digital health, and artificial intelligence, where the ethical and transparent handling of data becomes a critical adoption criterion.

In this context, GDPR compliance should not be understood solely as a legal obligation, but as an opportunity to build sustainable competitive advantages. Established companies such as Apple, Qwant, and Deutsche Telekom have integrated their privacy

structures as a fundamental part of their value proposition, using regulatory compliance as a differentiator against less transparent competitors or those with limited presence in regulated jurisdictions (Steppe, 2017; Sirur et al., 2018).

This challenge is intensified for early stage tech startups in the process of internationalization, which operate under pressure to scale quickly with structures still in development. Such is the case of Propulse, a startup founded in Peru that uses artificial intelligence models to detect real estate investment opportunities through predictive analysis of leads and identification of undervalued properties. In its expansion toward the European market, particularly Portugal, Propulse faces the challenge of aligning its technological, organizational, and legal model with the principles of the GDPR, without compromising its agility or its data driven value proposition.

This structural tension between regulatory compliance and the need to scale can, however, become a strategic opportunity if addressed from a proactive governance perspective. As authors such as Pagallo (2019) and Mühlhoff (2023) warn, integrating privacy practices, algorithmic ethics, and accountability from early stages not only facilitates legal compliance but also builds social legitimacy, strengthens competitive differentiation, and enables access to European innovation ecosystems that prioritize ESG standards and digital responsibility.

This research assumes that GDPR compliance can offer real strategic benefits to a tech startup in expansion. To that end, it analyzes how Propulse adapted its processes to the GDPR framework as part of its entry into the European market. A pilot developed

with the Portuguese modular housing company Litehaus is analyzed, which made it possible to validate best practices in informed consent, pseudonymization, internal auditing, and algorithmic transparency.

In addition, the research incorporates a comparative review of European cases, interviews with ecosystem experts, as well as an empirical exploration of the institutional, commercial, and technical impact of adopting the GDPR as an axis of organizational strategy. The aim is not only to assess Propulse's regulatory compliance but also its ability to position itself as a trustworthy, ethical, and innovative company in one of the most demanding regulatory environments in the world.

The objective is to provide a practical example of how data governance principles can become a tool for growth. The structure of this document is divided into seven chapters: Chapter 2 develops the theoretical framework on data governance, regulation, competitive advantage, and startups; Chapter 3 describes the applied qualitative methodology; Chapter 4 presents the empirical results; Chapter 5 discusses their relevance in the academic and business context; Chapter 6 outlines conclusions and recommendations; and Chapter 7 contains annexes and supporting materials.

2. THEORETICAL FRAMEWORK

2.1. The Evolution of the GDPR as a Regulatory Paradigm for Privacy

The General Data Protection Regulation (GDPR), approved in 2016 and in force since 2018, replaced Directive 95/46/EC and introduced stronger individual rights, proactive accountability, and uniform rules across all EU Member States, applying to any organization handling EU citizens' data, regardless of location. Its core principles include data minimization, transparency, purpose limitation, and the obligation to conduct Data Protection Impact Assessments (DPIAs).

Its influence has extended well beyond Europe. Countries like Brazil, Japan, and India have reformed their frameworks inspired by the GDPR, creating what Bradford (2020) calls the "Brussels effect." For startups like Propulse, research shows that embedding compliance early reduces future costs and builds institutional credibility with investors and partners (Gellert, 2018; Jin, Labadie & Legner, 2022), making the GDPR less a burden and more a framework for responsible growth..

2.2. Privacy as a Strategic Factor and Competitive Differentiator

In saturated digital markets, privacy has shifted from a legal obligation to a genuine competitive differentiator. Organizations that embed it into their strategy and culture do

more than avoid penalties, they build legitimacy, attract investment, and increase customer loyalty (ISACA, 2023; Gellert, 2018). Companies like Apple and Qwant have made privacy a core part of their commercial identity, positioning it as a feature rather than a compliance requirement.

At the technical level, privacy by design means building data protection into products from the start, not adding it later. This includes data minimization, pseudonymization, access controls, and transparent documentation for users (Cavoukian & Buerger, 2024; Mühlhoff, 2023). Research confirms that users are more willing to share data when they understand how it will be used and feel in control, which directly improves conversion, retention, and platform engagement (Creswell, 2021; Jin et al., 2022).

Beyond reputation, privacy has become a market access requirement. In public tenders and B2B agreements with regulated sectors, demonstrating GDPR compliance is often non-negotiable. Early adoption of governance structures, including a Data Protection Officer (DPO), internal policies, and accountability mechanisms, helps startups not just comply but compete (Ryngaert, 2020; Pagallo, 2019). A study of over 140 tech companies found that advanced GDPR compliance was linked to a 24% improvement in operational efficiency and stronger customer retention (Jin, Labadie & Legner, 2022), making privacy a concrete driver of business stability and growth

2.3. Data Governance as an Integrative Framework

Data governance is not just a compliance issue; it is a shared organizational responsibility that connects technical, legal, ethical, and strategic dimensions around how data is managed. According to Alation (2024), it encompasses the policies, structures, and technologies that enable data to be handled securely, efficiently, and in line with business objectives.

For startups like Propulse, where data underpins innovation, monetization, and AI-driven decision making, effective governance is especially critical. The GDPR provides a practical framework for this, combining principles such as data minimization, purpose limitation, and accountability with operational requirements like DPIAs, activity records, and the designation of a Data Protection Officer (DPO). These have been further institutionalized through standards like ISO/IEC 27001 and 27701 (GDPR Interoperability Model, 2021).

In practice, governance means embedding privacy by design into systems from the start, training teams, selecting vendors carefully, and monitoring processes continuously. As Gellert (2018) notes, effective governance must evolve alongside the company and its regulatory environment. It also carries an ethical dimension: with AI and automated decisions becoming central to many business models, principles of fairness, explainability, and human oversight are no longer optional (Mühlhoff, 2023). For Propulse, this has meant adapting its lead processing flow, auditing its algorithms, and ensuring traceability across the entire data lifecycle.

2.4. The Strategic Role of Privacy in Tech Startups

Tech startups often deprioritize privacy in the early stages, pressured by limited resources and the need to scale fast. This is a mistake. Evidence shows that embedding privacy from the outset leads to sustainable competitive advantages, especially in demanding markets like Europe (Pagallo, 2019; OECD, 2024).

Rather than reacting to compliance requirements, startups can use privacy by design as a proactive strategy. For Propulse, demonstrating GDPR compliance from the first commercial contact, through clear consent mechanisms, data traceability, and pseudonymization, has directly facilitated B2B sales and built credibility with potential clients.

Privacy also acts as a market filter. Startups that cannot demonstrate compliance are automatically excluded from public tenders, institutional investment rounds, and partnerships with global corporations. In this sense, getting privacy right is not just about protection, it is a strategic resource for accessing sophisticated markets and building lasting collaboration networks (Ryngaert, 2020; Jin et al., 2022).

2.5. Data Protection Impact Assessments (DPIA) and Algorithmic Governance

Article 35 of the GDPR requires organizations to conduct a Data Protection Impact Assessment (DPIA) whenever data processing is likely to pose a high risk to individuals' rights. For tech startups using AI and automated systems, this is not a formality but a practical tool for identifying and mitigating risks before they become problems.

Companies that implement DPIAs systematically report greater operational efficiency and lower reputational risk (Jin, Labadie & Legner, 2022).

For Propulse, DPIAs are especially relevant. Its business model relies on predictive models, automated lead categorization, and behavioral data processing, all of which carry real risks of bias, lack of transparency, or misuse. A well-executed DPIA helps identify which data are most sensitive, forces dialogue between technical and legal teams, and generates documentation that holds up in audits, B2B negotiations, and regulatory reviews.

Beyond compliance, DPIAs connect directly to algorithmic governance. As Mühlhoff (2023) argues, responsible AI requires anticipating not just how data is used today, but what decisions it will drive and what inequalities it might reinforce. Article 22 of the GDPR gives users the right to challenge decisions made solely by automated systems, which means Propulse must build explainability into its architecture, not as a legal afterthought, but as a foundation for user trust and institutional credibility.

2.6. Interoperability, International Standards, and Responsible Scalability

One of the core challenges of scaling a data-driven startup internationally is ensuring that systems from different countries and institutions can work together without compromising privacy or compliance. For Propulse, whose business model involves data flows across portals, CRM platforms, construction companies, and institutional

databases, interoperability is not a technical nicety but a operational necessity (GDPR Interoperability Model, 2021).

The most practical path forward is adopting established international standards. ISO/IEC 27001 and its privacy extension ISO/IEC 27701 provide recognized frameworks for designing and auditing governance systems, signaling to partners and regulators that processes are solid and certifiable (Houlihan Lokey, 2025). The GDPR Interoperability Model adds a layer of practical guidance, covering consent traceability, standardized metadata, secure APIs, and consistent rule enforcement across systems and borders.

For Propulse, early adoption of these standards does more than ensure compliance. It reduces future adaptation costs, strengthens positioning against competitors operating under looser regulatory environments, and makes the company a more credible partner in public procurement and institutional integrations. Interoperability, in this sense, is not just about making systems talk to each other. It is about building a foundation for responsible, scalable growth.

2.7. Data Ethics, Social Legitimacy, and Trust in Innovation

Data governance is as much an ethical issue as a technical or legal one. As public concern around personal data grows, the way a company manages and communicates its data decisions increasingly shapes how it is perceived, both by users and by the market (Gellert, 2018; Pagallo, 2019). Ethical data management means

acknowledging that algorithmic decisions can produce real consequences, including inequality and exclusion, and designing systems that account for this from the start.

For Propulse, this means going beyond privacy by design to embrace ethics by design: ensuring algorithms do not produce biases, that consent processes are genuinely understandable, and that users have a real way to question automated decisions (Mühlhoff, 2023). In practice, this involves plain language policies, detailed consent controls, bias minimization in models, and independent reviews of AI use.

This is not just about values. Companies that build responsibility into their services generate more stable relationships and are better positioned to weather regulatory or reputational pressure (Steppe, 2017; EDPLR, 2020). For Propulse, a strong data ethics posture strengthens its image with European clients and investors, opens access to ESG-focused funds, and becomes a genuine differentiator in an environment where transparency and fairness in technology are increasingly expected.

2.8. Conceptual Synthesis and Theoretical Framework Applied to Propulse

The previous sections show that data governance is far more than a compliance exercise. For a startup like Propulse entering the European market, the GDPR provides both a legal obligation and a practical roadmap for building a differentiated, trustworthy business.

Five principles frame the governance model proposed in this work:

a. The GDPR as a global structuring framework: it redefines how responsible innovation should be approached, particularly in sectors using AI and large-scale data processing.

b. Data governance as a bridge: connecting technical, legal, organizational, and social dimensions around how data is managed and communicated.

c. Privacy as a competitive advantage: in B2B contexts, meeting data protection standards is often a prerequisite for contracts, tenders, and partnerships with ESG-conscious institutions.

d. Ethical design and algorithmic auditing: building transparency, traceability, and explainability into products from the start strengthens credibility with clients, investors, and regulators.

e. Interoperability and international standards: adopting frameworks like ISO/IEC 27001, 27701, or the GDPR Interoperability Model enables scalable, legally sound expansion into new markets.

Table I, which closes this chapter, translates these principles into concrete actions and their strategic impact for Propulse, illustrating that good data governance is not a cost but a foundation for sustainable growth.

TABLE I

PRACTICAL APPLICATION OF THE GDPR IN TECHNOLOGY STARTUPS LIKE PROPULSE

GDPR Principle	**Technical Application in Propulse**	**Strategic Impact**
Data Minimization	Collect only the strictly necessary information from leads to operate AI models.	Lower legal risk, compliance with Art. 5 of the GDPR, and greater clarity for the user.
Transparency and Lawfulness	Implement a clear, accessible, and visible privacy policy, along with dynamic consent tools.	User trust, improved conversion rates, and positive brand perception.
Privacy by Design & Default	From the technical architecture: use pseudonymization, secure storage, access control, and user interfaces.	Validation with investors, reduced risk of future redesign, competitive advantage in tenders.
Impact Assessment (DPIA)	Conduct documented analyses on AI risks (bias,	Reduction of incidents and ability to demonstrate

	automated decisions, unauthorized access).	compliance to authorities or institutional clients.
Interoperability	Adopt ISO standards and the GDPR Interoperability Model to integrate with other platforms or entities.	Scalability to new countries/regions and credibility in technological integration processes.
Accountability	Document the entire data lifecycle, maintain access logs, assign roles, and conduct internal audits.	Strengthens reputation, improves internal processes, and facilitates future certifications.

3. METHODOLOGY

To analyze how the implementation of a data governance model can become a competitive advantage for Propulse within the framework of the General Data Protection Regulation (GDPR), a qualitative exploratory approach was chosen. This methodological choice responds to the complex nature of the phenomenon under study, which involves technical, regulatory, and cultural aspects inherent to a Latin American tech startup in the process of expanding to Europe.

Following Creswell (2021) and Yin (2018), the qualitative approach is especially useful when the goal is to understand not only what happens, but how and why it happens, considering the perspectives of the different actors involved. In this case, the interest was to examine how elements such as data ethics, *privacy by design*, and algorithmic governance are articulated within an emerging organization with international aspirations.

Rather than focusing exclusively on describing regulatory compliance, this methodology allowed for exploring how such compliance can be transformed into an organizational strategy with real impact. The inductive logic that guides this work facilitated the generation of insights based on the concrete experience of Propulse, as well as the interpretation of key specialists and users (Gellert, 2018; EDPLR, 2020).

The research was carried out in five interrelated phases, which allowed the construction, application, and validation of a governance model aligned with the GDPR and adapted to the company's operational reality.

3.1. Documentary Review and International Benchmarking

The first phase of the study consisted of a detailed review of relevant sources to build a solid theoretical and empirical foundation. Twenty seven documents were consulted (bibliography), including academic literature, European regulations, technical standards, and practical case studies of companies that have implemented advanced data governance models.

The literature search was conducted in databases such as Scopus, SSRN, Google Scholar, the European Data Protection Law Review (EDPLR), as well as documents published by the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), and the GDPR Interoperability Model (2021). Keywords used included: data governance, GDPR compliance, *privacy by design*, startups, algorithmic accountability, and interoperability.

Highlighted among the reviewed sources are:

- Official regulations and guides from the EDPB and EDPS.
- Academic studies such as Gellert (2018), Pagallo (2019), Steppe (2017), Ryngaert (2020), Sirur et al. (2018), Jin, Labadie and Legner (2022), and Mühlhoff (2023).

- International standards such as ISO/IEC 27001 and 27701.
- Reference business cases, including Apple, Qwant, Deutsche Telekom, MyHealth@EU, and N26.

All this information was organized into a matrix by dimensions (legal, technical, organizational, and ethical), allowing the identification of patterns and replicable best practices. This review not only contributed the theoretical framework for the study, but also served to design the analysis categories, interview questions, and the overall scheme of the governance model adapted to Propulse.

3.2. Propulse–Litehaus Pilot Study

In this phase, a pilot implemented by Propulse together with Litehaus, a Portuguese company that builds modular homes, was analyzed. The objective was to test the GDPR adapted data governance model in a real and controlled environment and observe its practical effects in different areas of the operation.

Over a four week period, concrete measures were applied, such as:

- Techniques of pseudonymization and data minimization in lead capture forms.
- Simulation of internal audits using the guidelines of ISO/IEC 27701.

To assess the impact, both quantitative and qualitative indicators were measured:

- Lead conversion rate before and after the pilot.
- Number of operational errors in data processing flows.

- Perception of the client (Litehaus) and the internal Propulse team regarding the new governance approach.

Data were collected using internal analytics tools, interviews with sales and legal leads, and direct feedback from the Litehaus team. This phase was key because it allowed for adjustments to parts of the model that were not viable in practice or that generated friction in the commercial process. It also reinforced the idea that integrating *privacy by design* can have concrete benefits in terms of efficiency and customer trust.

3.3. Semi-Structured Interviews with Experts and Key Stakeholders

The third phase involved conducting semi-structured interviews with eleven individuals with relevant experience in privacy, regulatory compliance, artificial intelligence, and the internationalization of startups to Europe. These interviews enriched the analysis with external perspectives and complemented what was learned during the pilot.

Profiles were selected using purposive sampling, prioritizing:

- Founders and CTOs of tech startups active in the European market.
- Lawyers specializing in data protection and compliance.
- Consultants in algorithmic ethics.
- Representatives from ESG focused accelerators.

The interviews were organized around five main topics:

- The strategic value of privacy in emerging companies.
- Common regulatory barriers for startups seeking internationalization.
- Practical cases of success or challenges in GDPR compliance.
- Internal auditing practices, interoperability, and the use of DPIAs.
- Reputation, investment, and competitiveness linked to compliance.

Some common patterns that emerged from these conversations included:

- The perception of the GDPR as a "natural filter" that excludes informal actors from the market.
- The growing importance of transparency and ethics in institutional procurement processes.
- The need to clearly explain how algorithms work, especially in B2B contexts.
- Proactive compliance as a factor that adds value in investment rounds or tenders.

These interviews offered a broader and more strategic view, helping to strengthen the governance model with insights that would not have emerged from within Propulse alone.

3.4. Participatory Design of the Data Governance Model

Based on the findings from the previous phases (document review, pilot, and interviews), a data governance model first draft was designed and adapted to Propulse's operational and cultural reality (founder cultural reality). Rather than imposing a rigid

structure, a participatory construction approach was chosen, directly involving the technical, commercial, and legal teams.

A collaborative work session (workshop) was held, applying tools such as *design thinking*, process mapping, and brainstorming. The objective was to identify critical points in data processing, assess compliance gaps, and propose realistic solutions aligned with GDPR principles.

Key outcomes of this process included:

- Creation of differentiated consent modules according to user type (client, agent, investor), with clear options and full traceability.
- Development of tailored templates for Data Protection Impact Assessments (DPIA) in the context of artificial intelligence.
- Implementation of internal dashboards to monitor governance indicators such as valid consent rates, processing errors, and response times to data subject requests.
- Definition of internal audit protocols and onboarding processes focused on *privacy by design* for new team members.

This process not only adapted the technical model to Propulse's real needs but also reinforced internal ownership of the issue. Several participants expressed that being actively involved in the design increased their commitment to GDPR compliance and their understanding of why going beyond legal obligations is important.

Furthermore, the final model was reviewed by two external specialists: a European DPO certified by EIPA and a Portuguese lawyer with experience in tech sector privacy. Both validated its technical and legal robustness and suggested specific improvements that were incorporated before concluding this phase.

3.5. Qualitative Analysis and Theoretical Empirical Integration

In this final phase, the findings from the previous stages were cross referenced with the concepts developed in the theoretical framework. The aim was to connect the data from the pilot, the interviews, and the participatory workshops with the most current academic approaches on data governance, privacy, and scalability in startups.

Some of the key connections that emerged were:

- Privacy as a strategic value: Both theoretically and practically, it became clear that sound data management is not just a legal obligation but a concrete way to build trust, reputation, and legitimacy, especially in markets like Europe.
- Traceability and consent as pillars of trust: The consent modules implemented in the pilot and the traceability dashboards aligned with the literature on privacy as a competitive differentiator.
- Interoperability and standards as enablers of growth: Interviews and reviewed documents emphasized that adopting frameworks like ISO 27001/27701 or the GDPR Interoperability Model allows startups to scale in an orderly and credible way.

- Algorithmic governance as an ethical commitment: Concerns about bias, explainability, and automated decision making were reflected across all sources. Incorporating internal audits, documenting decisions, and allowing human intervention became an aspirational standard for both Propulse and other organizations interviewed.
- Compliance as an organizational narrative: Several experts mentioned that compliance should not be seen only as an "external" requirement, but as part of the internal culture. This idea was reinforced during participatory workshops, where Propulse's teams integrated these principles into their daily routines.

Final Comments

Although the study is centered on a single company, efforts were made to ensure that the lessons learned would be transferable to other startups in similar situations. In fact, Propulse's experience could serve as a guide for many Latin American companies seeking to enter the European market and needing to adapt to the GDPR without losing agility or commercial focus.

Ethical Considerations and Limitations

Like all applied research, this work presents certain limitations that should be acknowledged:

- The analysis is based on a single case study (Propulse), which prevents statistical generalization of the results.
- The interviews did not include active representatives of regulatory entities such as Portugal's CNPD, which could have enriched the institutional perspective.

- The pilot was conducted under controlled conditions and did not face adverse situations such as real data breaches or legal disputes.

From an ethical point of view, a series of precautions were taken to ensure respect for the data and the people involved:

- All interviews and workshops were conducted under informed consent.
- The citations and analyzed logs were anonymized.
- No real personal data were used in the prototypes or tests conducted during the pilot.
- For each new process involving personal data, a preliminary impact assessment (DPIA) was prepared, in line with Article 35 of the GDPR.

In Table II: Methodological phases, applied techniques and relevance for Propulse, the phases are detailed along with a brief description of the technique used, references, and their application in Propulse.

TABLE II

METHODOLOGICAL PHASES, APPLIED TECHNIQUES AND RELEVANCE FOR PROPULSE

Phase	**Main Technique**	**References**	**Application in Propulse**

Documentary review and benchmarking	Systematic review and comparative analysis	EDPLR (2020), Jin et al. (2022), OECD (2024)	Identification of replicable good practices in privacy and data governance.
Propulse–Litehaus pilot study	Implementation and indicator analysis	Yin (2018), Gellert (2018)	Evaluation of the real impact of the proposed governance model on business operations.
Interviews	Semi-structured interviews	Creswell (2021), Pagallo (2019)	Gathering expert insights on privacy as a competitive advantage.
Participatory co-creation of the model	Workshops, design thinking, and mapping	Steppe (2017), Sirur et al. (2018)	Realistic and validated design of the data governance model.
Qualitative and theoretical triangulation	Integration of empirical evidence with theory	Ryngaert (2020), Mühlhoff (2023)	Conceptual consolidation of the framework applied to tech startups.

4. RESULTS

The results of this research show how the implementation of a data governance model focused on privacy, and aligned with the principles of the General Data Protection Regulation (GDPR), can generate real benefits in key areas for an expanding startup like Propulse. Through the empirical analysis conducted, it was possible to identify concrete improvements in commercial indicators, internal processes, and institutional perception. This section is divided into four parts:

- Analysis of the pilot implemented together with the Portuguese company Litehaus;
- Findings derived from interviews with experts and ecosystem actors;
- Validation of the proposed governance model;
- And a general synthesis of the most relevant lessons in relation to the literature.

4.1. Results of the Propulse–Litehaus Pilot

During the months of March and April 2025, Propulse developed a pilot with Litehaus, a Portuguese company dedicated to modular sustainable housing construction. The purpose was to test the data governance model designed to comply with the GDPR under real commercial operation conditions in a regulated B2B context.

Several measures were applied such as the integration of granular consent, data pseudonymization, improvements in traceability, and the adoption of *privacy by design* principles. These actions were implemented throughout the lead acquisition, management, and activation flow within Propulse's predictive system.

Quantitative Indicators

To evaluate the impact of these measures, key performance indicators (KPIs) were defined, whose results were:

- Lead conversion rate: increased from 12.5% to 13.1%, showing a modest but significant improvement in B2B environments.
- Leads discarded due to lack of explicit consent: reduced by 26%, thanks to improvements in data collection flows.
- Requests for data access or modification: increased by 43%, reflecting greater user awareness of their digital rights.
- Operational errors in data flows: decreased by 38%, suggesting an improvement in system stability and traceability.

Qualitative Findings of the Pilot

At a qualitative level, the pilot provided valuable lessons:

- The sales team noticed that conversations with potential clients were more fluid. The existence of clear privacy protocols from the first contact reduced legal barriers in the negotiation phase.

- Litehaus expressed a very positive assessment of the seriousness and professionalism shown by Propulse, highlighting its preparation in privacy matters as a differentiator compared to other providers.

4.2. Results of Interviews with Experts and Key Actors

As part of the methodological design, semi-structured interviews were conducted with various strategic profiles of the European ecosystem. Participants included founders of tech startups, data protection and compliance specialists, accelerator members, and professionals with experience in emerging technology regulation. The aim was to understand how privacy, GDPR compliance, and algorithmic governance are perceived from different positions.

The main findings are grouped into four broad categories:

a) Privacy as a Market Entry Barrier and Signal of Professionalism

A widely shared idea was that GDPR compliance acts as a sort of filter that distinguishes prepared startups from improvised ones. Several interviewees pointed out that, when evaluating partnerships, investments, or providers, a company with clear privacy protocols conveys maturity and seriousness.

An investor summarized it as follows:

«A startup that already has privacy sorted out enters with an advantage. It's like having passed a basic quality check before sitting down to negotiate.»

This view aligns with what Pagallo (2019) and Ryngaert (2020) propose, who describe the GDPR as a tool for structuring the digital ecosystem.

b) Privacy as a Commercial Differentiator

A second theme was the value of privacy as a competitive advantage. 70% of the experts interviewed mentioned that, nowadays, demonstrating compliance with norms such as the GDPR is essential to compete in sectors like health, fintech, or artificial intelligence. In particular, they emphasized its relevance in procurement processes, investment rounds, and negotiations with institutional clients.

A executive related with the CTO, mentioned:

«If you can't demonstrate you're GDPR compliant, you aren't even considered for certain contracts. It's not optional.»

This testimony reinforces what is discussed in the literature about early compliance as a lever for reputational positioning (Gellert, 2018; Jin et al., 2022; Houlihan Lokey, 2025).

c) Algorithmic Transparency and Automated Decisions

Many interviewees expressed concern about the opacity in the functioning of automated systems. In particular, they warned that decisions made by algorithms without the possibility of explanation or review generate distrust, both from an ethical and legal point of view.

Good practices mentioned included:

- Having traceability of algorithmic decisions.
- Guaranteeing human intervention in sensitive decisions.
- Providing users with the possibility to object to automated decisions (Art. 22 of the GDPR).
- Clearly documenting the criteria and thresholds used by the models.

In this regard, algorithmic transparency was seen not only as a duty but also as an opportunity for differentiation, especially in startups like Propulse, which use artificial intelligence as a central part of their value proposition. As Mühlhoff (2023) points out, ethical management of algorithms strengthens user trust and reduces the risk of regulatory or reputational questioning.

d) Data Ethics as a Valued Attribute by Investors

Finally, about 45% of interviewees highlighted that certain ethical behaviors, such as offering clear privacy policies, accessible language, and real user control options, are increasingly valued by accelerators, ESG focused funds, and large companies.

According to this group, these practices can tip the scales in favor of a startup in competitive selection or funding processes. This perspective is in line with Gellert (2018), Pagallo (2019), and EDPLR (2020), who understand data ethics as a new factor for institutional sustainability and legitimacy.

4.3. Empirical Validation of the Governance Model

To verify the strength and applicability of the data governance model developed for Propulse, a cross validation strategy was applied. This involved comparing the pilot's lessons, the perceptions collected in interviews, and the GDPR reference guidelines, supplemented with international standards and external validations. From this process, five dimensions emerged that confirm the viability and strategic value of the adopted approach.

a) Legal Alignment with the GDPR

Two specialists, one from Propulse's legal team and one external advisor, reviewed the model and concluded that it aligns with the main articles of the GDPR. In particular, they highlighted:

- The principle of transparency and lawfulness (Art. 5.1.a), implemented through accessible privacy notices and explicit consent.
- Data minimization (Art. 5.1.c) and purpose limitation (Art. 5.1.b), applied through optimized forms and lead pseudonymization.

- Accountability (Art. 5.2), with complete documentation of the data lifecycle and execution of DPIAs for AI based systems.

In addition, the experts stated that the model could be easily adapted to operate in other European countries, reducing the need for future redesigns and facilitating Propulse's international expansion.

b) Operational Effects and Internal Maturity

Operationally, the implementation of the model brought concrete benefits. For example:

- A data flow map was designed with clearly defined roles and permissions.
- Processes for obtaining and recording consent were standardized.
- Every new team member receives basic privacy training from their first day.

This not only helped reduce internal errors and response times but also professionalized operations in the eyes of third parties. The technical team reported improvements in traceability for tasks like support, debugging, and audits.

c) Impact on Commercial Perception

From a commercial perspective, the model helped position Propulse as a reliable and professional startup. Some concrete examples include:

- Inclusion of Propulse in the radar of European accelerators with explicit compliance requirements.
- A 12% improvement in B2B client response rates upon receiving clear information about how their data is managed.
- Recognition from Litehaus, who valued the legal and technical approach as a differentiator compared to other providers.

These elements suggest that, for many ecosystem actors, privacy is not just a legal requirement but a criterion that directly influences business decisions.

d) Technical Sustainability of the Model

An external software architecture specialist reviewed the technical design of the model and validated its robustness. Highlights include:

- The use of a modular architecture that allows components to scale without compromising privacy.
- The integration of a Consent Management Platform (CMP) that connects smoothly with CRM and analytics tools.
- The application of segmented access controls and automated pseudonymization.

These elements strengthen the system's resilience, facilitate audits, and allow for quick adaptation to regulatory changes or new technological alliances.

e) Institutional Transformation and Organizational Culture

Finally, the implementation process also had a positive effect on Propulse's internal culture. Observations included:

- Increased use of privacy and governance language in operational meetings.
- The spontaneous creation of a small cross functional committee that discusses ethical implications of new product features.
- Inclusion of privacy modules in onboarding and continuous training processes.

These changes indicate that data governance did not remain at a formal or documentary level but began to integrate into the company's daily life. As Steppe (2017) mentions, when an organization embraces privacy as a shared value, it strengthens its legitimacy with partners, investors, and clients.

4.4. Key Findings

The implementation of the data governance model and the associated empirical analysis made it possible to identify several lessons that confirm the hypothesis of this research. These findings provide a valuable foundation for future replications of the model in startups facing similar challenges:

- Clear privacy policies help convert more leads. When legal texts and forms are well explained and easy to understand, people are more willing to share their data. This resulted in a better conversion rate.

- Adapting to the GDPR from the beginning avoids problems later. Having everything in order from the start facilitated the sales team's work and avoided legal obstacles that previously slowed down sales or made it harder to close contracts.

- Privacy is seen as a sign of seriousness. Institutional clients and potential investors positively valued that Propulse had a clear data governance structure, which improved the company's overall image.

- Audits and impact assessments score points with demanding clients. Having DPIAs and internal records helped show that Propulse takes data protection seriously, which was well received by strategic partners and potential allies.

- Algorithmic governance increases transparency. Being able to explain how predictive models work and ensuring there are no fully automated decisions without human review was key to building trust, especially in sensitive sectors like real estate.

- Having interoperable systems improves efficiency. Secure and traceable integration of different platforms not only streamlined internal work but also facilitated demonstrating compliance to third parties.

- Pseudonymization protects data without affecting system functionality. Separating the lead's identity from their analyzed data reduced risks without hindering predictions.

- Involving the team in model design generated more commitment. Internal workshops and co-creation of the model helped the team better understand the reasons behind it and feel part of the process, reinforcing the sustainability of the approach.

- Compliance opens doors. Thanks to the model, Propulse was able to apply (and be considered) in calls from accelerators and European programs that require GDPR compliance from the outset.

- Good data governance boosts innovation. Far from being a burden, well managed privacy allowed Propulse to move more freely, think about new services, and explore alliances without fear of sanctions or scrutiny.

5. DISCUSSION

The results obtained throughout this research show that GDPR compliance, far from being merely a legal requirement, can become a strategic tool to strengthen customer trust and differentiate a company in a highly competitive environment. In the case of Propulse, applying a privacy focused governance model not only enabled compliance with European regulations but also yielded tangible benefits in terms of operational efficiency, perception of institutional maturity, and positioning in the European market.

One of the most relevant points concerns the direct relationship between good privacy practices and the positive perception of users and strategic partners. As suggested by studies from ISACA (2023), the OECD (2024), and the EDPB (2025), elements such as transparency, data traceability, or user control clearly influence the decision to share personal information. This relationship was also reflected in the pilot case with Litehaus, where a slight improvement was observed in the lead conversion rate. This behavior aligns with the findings of Jin, Labadie, and Legner (2022), who found that organizations that integrate *privacy by design* tend to improve both their internal efficiency and their relationship with customers.

The *privacy by design* approach applied by Propulse follows the recommendations of authors such as Cavoukian & Buerger (2024), regarding the inclusion of privacy from the early stages of any system's development. In practice, this translated into the use of algorithms that respect explicit consent, interfaces that clearly explain data usage, and

systems that allow users to control the information they share. These changes not only helped to comply with the law but also improved the user experience by making everything related to their data more understandable and accessible.

Important technical measures such as pseudonymization and data minimization were also incorporated. Both strategies are recognized by the European Data Protection Board as best practices to reduce risk in the processing of personal data. In the case of Propulse, these practices did not represent operational obstacles, on the contrary: they provided technical robustness, increased process traceability, and facilitated internal controls.

Another relevant finding is that regulatory compliance, when managed intelligently, can become a differentiating factor compared to other market players. This was confirmed by both the interviews conducted and the signs observed in the model validation. Propulse was perceived as a serious and trustworthy company by European actors, in part thanks to its structured approach to privacy. As noted by Gellert (2018) and Steppe (2017), in markets like Europe, the trust a company inspires is often more decisive than the technical sophistication of its product.

The use of tools such as Data Protection Impact Assessments (DPIAs), the adoption of ISO standards, and regular internal audits are part of advanced governance. Studies such as those by Jin, Labadie, and Legner (2022) have shown that these practices not only reduce risks but also improve operational efficiency. This reinforces the idea that investing in compliance can generate sustainable structural benefits over time, especially in contexts with clear rules like the European market.

Another interesting aspect is how Propulse approached governance as a collaborative process. Involving different areas of the company, from the technical team to legal personnel, allowed the model to be more realistic, functional, and aligned with the organization's culture. This participatory approach was also valued by the experts interviewed, who highlighted the importance of building technology from an ethical logic and not just a minimum compliance logic. As shown by Gellert (2018) and Sirur et al. (2018), this vision helps to consolidate a company's long-term legitimacy.

From a more practical point of view, properly addressing privacy did not limit Propulse's innovation. Rather, it guided it toward more sustainable solutions aligned with market expectations. The external validation of the model, as well as the interest of European accelerators, demonstrates that a well implemented privacy culture can be a gateway to new business opportunities. As noted in the report "Advances in Data Protection and Artificial Intelligence," in the coming years, the convergence between digital ethics and privacy will be a key differentiating criterion for products based on artificial intelligence.

On the other hand, Propulse's experience also shows that there is no single way to apply the GDPR. Each company must adapt the principles of data governance to its specific reality, considering its size, level of technological maturity, available resources, and organizational culture. In this sense, rather than adopting a standard model, it is about building a custom model that makes sense for the business and can be sustained over time without compromising agility or competitiveness.

Finally, the model developed by Propulse can serve as a reference for other startups beginning their internationalization process toward regulated markets. Although each case has its own particularities, the processes, tools, and learnings documented in this study demonstrate that it is indeed possible to transform a legal requirement into a strategic advantage if there is commitment from leadership, a long-term vision, and a culture of continuous learning.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1. Conclusions

This work has shown that personal data protection is not only a legal obligation but can become a true strategic lever for tech startups aiming to grow in markets like Europe. Through the case of Propulse, it was validated with concrete evidence that actively complying with the General Data Protection Regulation (GDPR) not only avoids penalties but also brings real value in terms of reputation, efficiency, and business results.

Designing and implementing a data governance model adapted to Propulse's specific context led to several positive outcomes:

- Lead conversion improved and commercial cycle times were shortened.
- Greater trust was generated among institutional clients and potential investors.
- Key internal processes were organized, facilitating traceability and audits.
- Principles of algorithmic ethics were incorporated from early development stages.
- External perception of the company's organizational maturity was elevated.

In summary, when a company manages its data well, it not only complies with regulations but also gains ground in its sector.

However, this process does not happen on its own. It requires leadership, commitment, and collaboration between different areas of the organization. It also demands a vision that sees regulatory compliance not as a burden but as an opportunity to build legitimacy and differentiation. Throughout the study, both the pilot developed with Litehaus and the interviews with European experts confirmed that startups that take privacy seriously from the start are better positioned to grow, attract investment, and consolidate in regulated environments.

Additionally, the use of tools such as Data Protection Impact Assessments (DPIAs), consent management platforms, or internal audits not only serve to "cover" regulatory requirements. They also contribute to improving product quality, increasing user trust, and strengthening relationships with strategic allies.

The Propulse experience shows that adopting standards such as ISO/IEC 27701 or following guidelines like the GDPR Interoperability Model is possible, even for small startups. Far from slowing innovation, these best practices provide structure, strengthen institutional reputation, and open doors in spaces that value compliance and digital responsibility.

On an organizational level, it became clear that data protection is not solely the concern of the legal or technical team. It must be integrated into the company's overall strategy. In the case of Propulse, working jointly across departments and building a model adapted to its reality enabled the development of a strong privacy culture, with clear

procedures, defined metrics, and continuous internal training. This institutional maturity is key to sustainable growth.

Moreover, it was confirmed that privacy can be a brand differentiator. In environments where personal data is increasingly valuable and sensitive, showing ethical commitment and transparency has become a highly appreciated value. For startups looking to compete with major players or enter public contracts, this approach can make a difference.

6.2. Recommendations

Based on the insights gained from this research, the following recommendations are proposed for both Propulse and other tech startups seeking to enter or establish themselves in highly regulated markets like Europe:

- Incorporate *Privacy by Design*. From the start of product and service development, it is essential to consider privacy principles. This includes defining legal requirements early, using technologies such as pseudonymization or encryption, and ensuring traceability in each data flow. Doing so early avoids costly fixes later and projects a responsible image to third parties.
- Conduct Regular Impact Assessments (DPIAs). DPIAs should not be seen as bureaucratic procedures but as tools that help anticipate risks, make better decisions, and demonstrate responsibility to clients and regulators. Integrating

them into the software development cycle strengthens internal compliance culture and avoids surprises in future audits.

- Communicate Compliance as a Competitive Advantage. Good privacy practices should be actively showcased, not just silently complied with. Including these elements in commercial presentations, sales processes, tenders, and institutional materials helps generate trust and open new business opportunities. Compliance also sells.

- Build Multidisciplinary Teams. It is crucial that the company does not delegate privacy to a single profile or department. Ideally, teams should combine technical, legal, and ethical knowledge. Investing in training or having specialized advice (e.g., from European DPOs) can make a big difference in decision quality.

- Adopt Standards and Enable Interoperability. Standards like ISO/IEC 27701 or the GDPR Interoperability Model are not just for large corporations. Applying them from the beginning allows startups to prepare for scaling, collaborate with more demanding partners, and present themselves in international calls with greater credibility.

- Promote Active Participation in Privacy Policy Building. Including users, strategic allies, and experts in policy definition not only improves quality but also strengthens the legitimacy of the developed solutions. This participatory approach also facilitates long-term relationships based on mutual trust.

- See Privacy as an Investment, Not a Cost. Changing the mindset is key. Investing in privacy and data governance is not just about avoiding fines but about building a stronger, more reliable company ready to grow. In an environment where trust is a scarce asset, protecting data becomes a clear competitive advantage.

7. REFERENCES

Alation. (2024). Data Governance and Trust. Alation Whitepaper.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Cavoukian, A., & Buerger, D. (2024). *Privacy by Design* in AI Systems. ACM Journal.

Creswell, J. W. (2021). Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 4th Ed. SAGE Publications.

Davenport, T. H. (2024). Competing on Analytics. Harvard Business Review Press.

EDPB. (2025). GDPR Enforcement Overview 2025. European Data Protection Board.

EDPLR. (2020). European Data Protection Law Review, 6(3), 263–272. https://doi.org/10.21552/edpl/2020/3

Eurostat. (2025). Digital Economy and Society Statistics. Publications Office of the European Union.

GDPR Interoperability Model. (2021). Technical Guidelines on Data Portability and Interoperability. European Commission.

Gellert, R. (2018). Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative. Computer Law & Security Review, 34(2), 222–228. https://doi.org/10.1016/j.clsr.2017.11.003

Houlihan Lokey. (2025). PropTech Industry Annual Review 2024. Sector Report.

ISACA. (2023). Privacy in Practice 2023. ISACA Global Research.

Jin, X., Labadie, J., & Legner, C. (2022). Data Protection Regulations and Digital Innovation: Empirical Evidence from the GDPR. Journal of Strategic Information Systems, 31(2), 101733. https://doi.org/10.1016/j.jsis.2022.101733

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2018). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. SAGE Publications.

Mühlhoff, R. (2023). *Predictive Privacy*: Towards an Ethics of Algorithmic Inference. AI & Society, 38, 267–284. https://doi.org/10.1007/s00146-022-01529-y

OECD. (2024). Data Privacy as Competitive Advantage. OECD Digital Economy Report. https://www.oecd.org/sti/data-governance

Pagallo, U. (2019). Advanced Introduction to Law and Artificial Intelligence. Edward Elgar Publishing.

PropTechMap. (2024). 2024 Landscape of Property Technology Startups in Europe. https://www.proptechmap.com

Ryngaert, C. (2020). The Governance of Data in the European Union: A Normative Assessment of the GDPR. European Journal of International Law, 31(1), 243–272. https://doi.org/10.1093/ejil/chaa010

Sartor, G., & Lagioia, F. (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. European Parliamentary Research Service. https://doi.org/10.2861/293

Sirur, S., Nurse, J. R. C., & Webb, H. (2018). Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, 88–95. https://doi.org/10.1145/3267357.3267366

Steppe, R. (2017). Data Protection and Startups: A Strategic Perspective. Information Systems Journal, 27(6), 755–778. https://doi.org/10.1111/isj.12123

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods, 6th Ed. SAGE Publications.

8. ANNEXES

Annex I: Technical Glossary

Accountability (Proactive Responsibility):

A core principle of the GDPR (Art. 5.2) requiring organizations not only to comply with data protection rules but also to be able to demonstrate such compliance. In the case of Propulse, this translates into continuous documentation, internal audits, and clear role assignments.

Data Protection Impact Assessment (DPIA):

A mandatory evaluation when data processing may involve a high risk to individuals' rights and freedoms. It includes risk identification, mitigation measures, and decision documentation. Fundamental for AI using startups like Propulse.

Algorithmic Audit:

A technical and ethical review process of automated decision making models. It assesses whether there are biases, lack of transparency, or unintended effects in the use of algorithms. May include internal tests, explainability, and external validation.

Granular Consent:

An advanced form of consent that allows the user to accept or reject data processing for specific purposes (e.g., marketing, analytics, profiling). It is key to complying with transparency and user autonomy principles.

Consent Management Platform (CMP):

A technological tool that manages the collection, storage, and traceability of user consent. Its integration in Propulse facilitated GDPR compliance and reduced lead rejection.

Data Governance:

A set of policies, processes, structures, and technologies that enable data management in an ethical, legal, secure, and efficient manner. In this thesis, it is considered a strategic, technical, and reputational axis for tech startups.

Data Minimization:

A principle stating that only strictly necessary data should be collected for the intended purpose. In Propulse, this means excluding irrelevant information from predictive models.

Data Portability:

The user's right to receive their personal data in a structured format and transfer it to another provider. It has important technical implications for system interoperability.

Data Protection Officer (DPO):

A role required by the GDPR in certain organizations, responsible for supervising data protection strategy and compliance. Although not mandatory for Propulse, appointing an internal responsible party is recommended.

GDPR (General Data Protection Regulation):

Regulation (EU) 2016/679, in effect since May 2018, which governs personal data protection in the European Union. It establishes rights for citizens and obligations for organizations, with extraterritorial reach.

Algorithmic Governance:

An ethical and technical management framework for algorithms that process personal data or make automated decisions. It involves transparency, explainability, review, and ongoing documentation. Relevant in contexts where AI is applied, as in Propulse.

Interoperability:

The ability of different systems and organizations to exchange and use information effectively, securely, and in compliance with regulations. Technical and semantic interoperability is key for startups operating across jurisdictions or sectors (e.g., proptech, e-health).

ISO/IEC 27001 – ISO/IEC 27701:

International standards for information security and privacy management, respectively. Recommended standards for startups seeking certification of their practices and strengthening their reputation with third parties.

Pseudonymization:

A process in which personal data is separated from direct identifiers, making attribution more difficult without additional information. Unlike anonymization, it remains regulated under the GDPR. It is useful for training predictive models without exposing sensitive data.

Privacy by Design **and by Default:**

Principles stating that privacy must be integrated from the initial system design and set by default in its configuration. In Propulse, this translates to interface design, AI models, and protocols that prioritize personal data protection.

Right to Explanation:

The user's right to understand the reasoning behind an automated decision that significantly affects them. Although legally debated, it is an increasing expectation in markets like the EU. Applicable to algorithms used in lead classification.

Annex II: Interview Matrix

Summary of interviewee profiles for the study on data governance and GDPR compliance in tech startups.

TABLE III

SUMMARY OF INTERVIEWEE PROFILES

No.	**Interviewee profile**	**Role/position**	**Type of institution**	**Country**	**Area of expertise**	**Approx. date**
1	Proptech startup founder	CEO	Tech company	Peru	International expansion and compliance	12/02/2025
2	Privacy law specialist	Senior legal consultant	Law firm	Portugal	Digital law and data protection	15/02/2025
3	Institutional investor	Partner	ESG investment fund	Portugal	Legal due diligence and digital reputation	19/02/2025

4	Accelerator representative	Program director	ESG focused accelerator	Portugal	Startup scalability and compliance	21/02/2025
5	Academic researcher	Professor and consultant	University & EU think tank	Peru	Data ethics and responsible AI	27/02/2025
6	AI legal advisor	AI & Privacy specialist	International law firm	Portugal	Algorithmic governance and GDPR	01/03/2025
7	Litehaus representative	Head of operations	Modular construction company	France	B2B tech integration and privacy	09/03/2025

Annex III: Semi-Structured Interview Guide

General Objective:

To explore how experts and key actors in the tech ecosystem perceive GDPR compliance, its impact on startups like Propulse, and its potential as a competitive advantage in regulated markets.

Interview Format:

- Duration: 30 to 50 minutes
- Platform: Zoom or Google Meet
- Language: based on interviewee preference (Spanish, Portuguese, or English)
- All interviews were recorded with verbal informed consent

Blocks and Questions:

1. Privacy as a Strategic Value

- How important do you think data privacy is today in tech startups?
- Have you seen cases where privacy really made a difference against competitors?
- How does privacy management affect a startup's reputation or credibility?

2. Challenges in GDPR Compliance

- From your experience, what are the main challenges startups (especially Latin American ones) face when trying to comply with the GDPR?

- Which parts of the regulation tend to be the hardest to implement?
- What common mistakes do you see in these processes?

3. Best Practices and Learnings

- Have you worked with or known startups that used GDPR compliance as a tool for growth?
- What do you think they did well?
- Is there any concrete practice you'd recommend to a startup beginning to internationalize?

4. Ethics, AI, and Automated Decisions

- What's your view on the use of AI in processes involving important decisions about people?
- Do you think legal compliance is enough, or should there be more in terms of ethics?
- What do you think about tools like DPIAs or human review mechanisms in automated decisions?

5. Advice for Expanding Startups

- If a Latin American startup wants to operate in Europe, what would you recommend they do from the beginning?
- Is it worth investing in GDPR compliance as part of their value proposition?
- Which standards or international frameworks do you think add value with European clients or partners?