الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

GRADUATION DISSERTATION

To obtain a Professional Master degree

« In Marketing Management »

THE IMPACT OF DATA PROTECTION LAWS COMPLIANCE ON CUTOMER LOYALTY
Case study : LAW 18/07, Saa assurances

Submitted by:

BELKHIRI HOUDHEIFA ABDERRAHMENE

BEGHOURA MOUAD

Supervised by:

Pr.DERRARE HACENE

Dr.NEDIL LAMIA

Academic year 2024/2025

Abstract

This thesis investigates the impact of personal data protection laws particularly
The Law 18/07 in Algeria on customer loyalty. It explores the mediating roles of trust and satisfaction in this relationship. Using a quantitative methodology based on a survey, the study analyzes how compliance with data protection regulations influences consumers' perceptions and loyalty behavior. Findings indicate that legal compliance enhances both trust and satisfaction, which in turn foster customer loyalty. The study highlights the strategic importance of data privacy compliance in marketing practices, especially in digital service sectors.

Key words: personal data, data protection, compliance, loyalty, satisfaction, trust.

Résumé

Ce mémoire étudie l'impact des lois sur la protection des données personnelles notamment la loi 18/07 en Algérie sur la fidélité des clients. Il explore le rôle médiateur de la confiance et de la satisfaction dans cette relation. À travers une méthodologie quantitative basée sur un questionnaire, l'étude examine dans quelle mesure la conformité aux réglementations sur les données influence les perceptions des consommateurs et leur comportement de fidélité. Les résultats montrent que la conformité aux lois améliore la confiance et la satisfaction des clients, qui, à leur tour, renforcent leur fidélité. L'étude met en lumière l'importance stratégique du respect des règles de protection des données dans les pratiques marketing, particulièrement dans les services numériques.

Mots-clés : Données personnelles, Protection des données, Conformité, Fidélité, Satisfaction, Confiance

ملخص

تَسْتَهدِف هذه الدراسة استكشاف تأثير قوانين حماية البيانات الشخصية لا سيما اللائحة العامة لحماية البيانات (GDPR) في أوروبا والقانون رقم(07-18) في الجزائر على مستوى ولاء العملاء. تتناول الدراسة دورَي الثقة والرضا كوسيطَين أساسيَّين في هذه العلاقة. اعتمادًا على منهجيَّة كمية مبنية على استبيانٍ موجه، تُقيِّم الدراسة مدَى تأثير التزام الشركات بالمعايير التنظيمية للبيانات على تصوُّرات المستهلكين وسلوكياتهم الولائية. وتشير النتائج إلى أن الامتثال لهذه القوانين يعزِّز شعور العملاء بالأمان والثقة، ويُفضِي إلى زيادة مستوى رضاهم؛ وهو ما ينعكس بدوره على تعزيز ولائهم للعلامة التجارية. في ضوء ذلك، تؤكد الدراسة أهمية الالتزام الصارم بقواعد حماية البيانات كاستراتيجية تسويقية حيوية، خاصةً في قطاع الخدمات الرقمية.

.

Acknowledgements

First and foremost, we bow in gratitude to our Almighty Creator, **ALLAH**, for His boundless mercy, for guiding us through every difficulty, and for granting us the strength, patience, and perseverance to bring this journey to an end. Every moment of doubt, every challenge we faced, was met with His light and for that, we are eternally thankful.

This work is far more than just the outcome of our academic efforts; it is the result of a shared journey filled with learning, growth, and the immeasurable support of those around us.

With heartfelt emotion, we express our deepest thanks to **Mm.Nedil**, whose wisdom and kindness illuminated our path. Her guidance was more than professional, it was human, empathetic, and inspiring. Her belief in us gave us the confidence to keep going when the road felt uncertain.

To **Professor Derrare Hacene**, thank you for your attentiveness, your encouragement, and your dedication to helping us see beyond the surface. Your presence brought clarity, and your mentorship left a lasting impact.

We would also like to express our profound gratitude to **Mr. Bilal Mazouzi**, Commercial Director of SAA, for his generous support and valuable contributions to this project. His availability, trust, and sincere interest in our work reminded us that collaboration and kindness go hand in hand in the professional world.

To our beloved families words will never be enough. You are the heart behind every page of this thesis. To our parents: thank you for your infinite love, your sacrifices, your prayers whispered late at night, and your faith in our dreams. You taught us strength through silence and courage through compassion. Your unwavering support gave us wings.

To our siblings thank you for your patience and for making us feel grounded, loved, and supported even in the most stressful times. You made us laugh when we needed it the most, and you reminded us of who we are beyond the academic pressures.

To our friends, who became our second family, thank you for walking beside us through every step of this journey, to those whose names we carry in our hearts: your jokes, your support, your late-night talks, and your constant presence brought joy and strength into our lives. We are so lucky to have shared this time with you.

To my Partner more than just a partner in work, you were a true companion in this adventure. We lifted each other when one fell, celebrated the little victories, and never stopped believing in the bigger picture. I could not have asked for a better teammate.

In closing, this thesis is not just an academic project it is a story of gratitude, resilience, and deep human connection. It stands as a tribute to all those who have walked with us, held our hands, and cheered us on from the sidelines. We carry your love and kindness with us, always.

Thank you. From the depths of our hearts.

Tables of continent

List of figures

List of tables

List of Abbreviations and Acronyms:

ANPDP: National Authority for Personal Data Protection.

AZOP: Croatian Personal Data Protection Agency.

APDP: Data Protection Authority (Francophone).

CCAP: Commission for the Control of Protection Activities.

CNDP: National Commission for Data Protection.

CNIL: French Data Protection Authority.

DDBM: Data-Driven Business Models.

DPD: Data Protection Directive.

DIR95: Directive 95/46/EC.

DPOS: Data Protection Officers.

EDPB: European Data Protection Board.

GDPR: General Data Protection.

LGPD: Brazilian General Data Protection Law Regulation.

OECD: Organization for Economic Co-operation and Development.

PETS: Privacy-Enhancing Technologies.

INTRODUCTION

The rapid digitization of global economies and societies has necessitated a robust regulatory response to address the escalating risks of personal data exploitation, prompting governments worldwide to enact stringent privacy laws designed to balance innovation with individual rights. Landmark frameworks such as Europe's General Data Protection Regulation (GDPR), Algeria's Law No. 18-07 on personal data protection (2018), California's Consumer Privacy Act (CCPA), and Brazil's General Data Protection Law (LGPD) exemplify this paradigm shift toward prioritizing transparency, accountability, and user consent in data governance. Building on foundational efforts like the EU's 1995 Data Protection Directive, these modern regulations establish universal principles such as explicit consent, data minimization, and purpose limitation, while adapting to regional contexts.

For instance, Algeria's Law 18-07, enforced by the Autorité de Protection des Données Personnelles (APDP), mandates strict oversight of cross-border data transfers and aligns with global standards like the GDPR, while addressing local concerns such as safeguarding citizen data in emerging digital markets. Extraterritorial provisions within these laws further compel multinational corporations to comply regardless of their geographic base, penalizing breaches with fines proportional to revenue to deter non-compliance.

While such regulations disrupt traditional marketing practices such as invasive profiling and unchecked third-party data sharing, they also drive innovation in privacy-preserving technologies, including advanced anonymization tools, blockchain-based consent management systems, and zero-knowledge verification protocols. Scholars argue that these laws play a dual role: challenging industries to abandon exploitative data practices while fostering ethical frameworks that prioritize long-term consumer trust. (Al-Fayad, 2020)

However, tensions persist, particularly for small and medium enterprises (SMEs) grappling with compliance costs and the "privacy-personalization paradox," where consumers demand both tailored services and absolute control over their data. Collectively, these regulations mark a transformative era in data governance, redefining privacy not merely as a legal obligation but as a cornerstone of sustainable innovation and consumer empowerment in the digital age.

Research question:

Based on the context outlined above, the central research question for this study is phrased as follows:

How does compliance with data protection laws impact customer loyalty, with trust and satisfaction acting as mediators?

Derived from this primary research question, a set of secondary questions has been developed to provide a more structured roadmap for the exploration and analysis undertaken in this research. These secondary inquiries enable a more detailed investigation of the main question, offering a framework for deeper examination and understanding of the complex dynamics between legal compliance, customer perceptions, and loyalty behaviors within the context of modern data governance.

The sub-questions are formulated as follows:

- **What is the impact of compliance with data protection laws on customer loyalty?**

  This question aims to investigate whether organizations' adherence to privacy regulations such as the Algeria's Law 18-07 can positively or negatively affect customers' long-term commitment and loyalty toward a brand or service provider.

- **How does compliance with data protection laws influence customer trust and satisfaction?**

  This sub-question seeks to explore the extent to which compliance efforts affect the trust customers place in organizations and their satisfaction with the service experience, considering that perceptions of data security and respect for privacy are increasingly critical to customer relationships.

- **How do trust and satisfaction mediate the relationship between compliance with data protection laws and customer loyalty?**

  This final sub-question seeks to examine the mediating role of trust and satisfaction in translating legal compliance into customer loyalty. It aims to determine whether improving customer trust and satisfaction, as a result of rigorous compliance practices, ultimately leads to stronger loyalty among consumers.

  Understanding this mediation mechanism would provide valuable insights for organizations seeking to align their data protection strategies with long-term customer relationship management goals.

Objectives of the research

This research aims to explore the intricate relationship between compliance with data protection laws, customer trust and satisfaction, and customer loyalty in order to:

- Identify the effect of compliance with data protection laws on customer loyalty:
  The study seeks to determine the extent to which adherence to privacy regulations, such as the GDPR and Algeria's Law 18-07, influences customer loyalty toward brands and service providers.
- Determine the influence of compliance with data protection laws on customer trust and satisfaction:
  This objective focuses on examining whether organizational compliance with data protection standards significantly enhances customer trust and satisfaction by reinforcing perceptions of transparency, accountability, and respect for personal data.
- Establish the relationship between customer trust, satisfaction, and customer loyalty:
  After understanding the individual impacts of trust and satisfaction, the research aims to uncover the nature of their relationship with customer loyalty, particularly how positive perceptions fostered through compliance can strengthen long-term consumer commitment.
- Examine the mediating role of trust and satisfaction in the relationship between compliance with data protection laws and customer loyalty:
  The final objective is to explore whether trust and satisfaction act as mediating variables, serving as mechanisms through which compliance with data protection laws translates into higher levels of customer loyalty.

Hypothesis

Taking into account the selected conceptual model and the insights gathered from the literature review, we have formulated hypotheses that describe the relationships between the variables in this study. Specifically, we hypothesize that compliance with data protection laws has a positive impact on customer loyalty, with customer trust and satisfaction acting as mediating factors.

In order to address the central research question of this study, and building on the works of relevant scholars (Zhang et al., 2020) we seek to explore how compliance with data protection laws influences customer loyalty through the mediating roles of customer trust and satisfaction. The following hypotheses are proposed:

Main Hypothesis
H0:
Compliance with data protection laws positively impacts customer loyalty.

Sub-Hypotheses
1. The effect of compliance on trust and satisfaction:
H1:
Compliance with data protection laws positively affects both customer trust and satisfaction,.

2. The effect of customer trust and satisfaction on loyalty:
H2:
Customer trust and satisfaction both positively influence customer loyalty.

3. Customer Trust and Satisfaction as Dual Mediators between Data Protection Compliance and Loyalty
H3: Customer satisfaction and customer trust jointly mediate the positive relationship between compliance with data- protection laws and customer loyalty.

Methodology:

To address the established research problem, this study adopts an empirical approach based on a quantitative research methodology. A survey will be conducted on a representative sample of the study population to gather data. This methodology is particularly suited to examine the impact of compliance with data protection laws on customer loyalty, with a focus on customer trust and satisfaction as mediating factors. The choice of this approach allows us to analyze the influence of regulatory compliance on customer loyalty, while exploring the mediating roles of trust and satisfaction in this relationship.

Announcement of the plan

The present work is organized into several chapters, each contributing to the progression and coherence of the overall research process.

- The **Introduction** sets the stage by presenting the general context and the importance of the research theme. It specifies the objectives pursued by the study, formulates the central research problem, and outlines the key hypotheses to be tested. This section also highlights the relevance of the subject in the current scientific and professional landscape.
- **Chapter I** is devoted to building the theoretical framework necessary for understanding the research topic. It is divided into two main sections. The first section provides a comprehensive literature review, synthesizing previous empirical studies and theoretical contributions related to the research variables. The second section proposes the conceptual framework, including the definition of concepts the relationships between variables, and the formulation of the research model guiding the study.
- **Chapter II** presents the methodological framework adopted to carry out the study. It includes a description of the research design, the data collection methods, the tools used, and the sampling techniques. This chapter also introduces the host organization in which the empirical study was conducted, offering insight into its structure, activities, and relevance to the research topic.

- **Chapter III** is dedicated to the presentation and analysis of the results obtained from the quantitative study. It begins with the statistical processing of the collected data and then discusses the main findings in light of the research hypotheses and theoretical expectations. The discussion highlights both consistencies and discrepancies with previous work, providing a critical interpretation of the results.
- Finally, the **Conclusion** offers a synthesis of the main insights gained from the study. It summarizes the key findings, evaluates the achievement of the research objectives, and reflects on the limitations encountered during the investigation. The chapter concludes by suggesting practical implications and outlining avenues for future research that could deepen or broaden the understanding of the topic.

CHAPTER I: THEORITICAL FRAM

SECTION 1: literature review

As digital ecosystems expand, governments worldwide have introduced a wave of data privacy laws from Europe's GDPR and Algeria's Law 18-07 to California's CCPA and Brazil's LGPD to safeguard personal information in an increasingly connected world.

These regulations, building on earlier frameworks like the EU's 1995 Data Protection Directive, prioritize transparency, accountability, and individual control. For instance, Algeria's Law No. 18-07 of 2018 establishes principles such as explicit consent, data minimization, and oversight by the Autorité de Protection des Données Personnelles (APDP), aligning with global standards while addressing local needs.

Globally, such laws mandate explicit consent, limit data collection to necessity, and enforce penalties for breaches, with extraterritorial rules requiring compliance even for firms outside regulated jurisdictions. While these laws disrupt traditional data practices (e.g., invasive profiling, cross-border data flows), they also drive innovation in privacy-preserving technologies like anonymization tools and blockchain systems. Research underscores their dual role: challenging industries to adapt while fostering ethical frameworks that prioritize long-term consumer trust (Al-Fayad, 2020).

1.1 Regulation's impact on marketing strategies and innovation

The introduction of the GDPR has fundamentally altered the landscape of digital marketing. Businesses have had to rethink how they collect, store, and leverage consumer data while maintaining compliance.

Expanding on this The European Union's General Data Protection Regulation (GDPR), enacted in 2018, and has fundamentally reshaped data-driven marketing strategies by imposing stringent requirements on data collection, processing, and consumer consent. Replacing the Data Protection Directive (DPD), GDPR emphasizes transparency, accountability, and individual rights, mandating explicit consent for data usage, anonymization of personal information, 72-hour breach notifications, and the appointment of Data Protection Officers (DPOs) (Hoofnagle et al., 2019).

Building further these regulations directly challenge marketing practices reliant on big data, which traditionally leverage vast, granular datasets for personalized campaigns, dynamic pricing, and predictive analytics *(*Akter & Wamba, 2016).

Key GDPR provisions such as the “right to erasure” (Article 17) and restrictions on automated decision-making (Article 22) limit marketers’ ability to harness identifiable consumer data, forcing firms to recalibrate strategies around anonymized or pseudonymized datasets. While big data applications like Netflix’s recommendation algorithms or Amazon’s demand forecasting thrive on detailed consumer insights, GDPR’s anonymization requirements reduce data specificity, complicating personalized marketing.(Camilleri, 2019)

Additionally, GDPR’s extraterritorial scope (Article 45) compels global firms to comply when handling EU citizens’ data, increasing operational costs and necessitating infrastructural overhauls. Emerging technologies like blockchain offer promising solutions, enabling decentralized, encrypted data management that aligns with GDPR’s privacy-by-design principles while restoring consumer control through mechanisms like tokenized consent.

(Wirth & Kolain, 2018)

Despite initial concerns about stifling innovation, GDPR has spurred advancements in privacy-preserving analytics, such as Next Best Action (NBA) strategies that utilize real-time, aggregated data to anticipate consumer trends without compromising individual privacy. The regulation also incentivizes ethical data monetization models, such as direct consumer compensation for data sharing, balancing compliance with competitive advantage. Overall, GDPR represents a pivotal shift toward ethical data governance, compelling marketers to prioritize transparency and consumer trust while navigating the evolving intersection of big data utility and regulatory compliance

In parallel, Requicha et al. (2021) explore the transformative impact of the General Data Protection Regulation (GDPR) on digital marketing, analyzing how organizations must adapt to subjective obstacles such as explicit consent requirements, data transparency, and compliance costs. The study emphasizes GDPR’s role in reshaping marketing strategies through mandates like granular consent management, "data protection by design," and the appointment of Data Protection Officers (DPOs). By examining case studies, such as BMW’s GDPR-compliant email campaigns achieving a 61.67% open rate, the authors highlight how compliance fosters trust and engagement by targeting consenting audiences. However, challenges include reduced database sizes due to stricter consent rules, increased costs for paid advertising (e.g., higher click prices on platforms like Google and Facebook), and operational complexities in managing cross-border data transfers. The study also identifies contradictions: while GDPR disrupts traditional data-driven tactics (e.g., cookies

and remarketing), it incentivizes ethical practices, urging firms to prioritize inbound marketing, SEO, and transparent communication. Ultimately, GDPR is framed as both a regulatory hurdle and a catalyst for innovation, driving long-term gains in customer loyalty and brand reputation. Key Terms: GDPR, Consent Management, Data Portability, DPO, Ethical Marketing, Inbound Marketing.

Similarly, Al-Fayad (2020) examines the General Data Protection Regulation (GDPR)'s transformative impact on data-driven marketing strategies, emphasizing its shift from the 1995 Data Protection Directive (DPD) to stricter mandates like explicit consent, data anonymization, and breach notifications. The study reveals that GDPR challenges traditional big data practices by reducing personalization capabilities (e.g., targeted ads, loyalty programs) and increasing compliance costs, while driving innovation through block chain technologies (e.g., Brave Browser, Block stack) that decentralize data control and enhance privacy. The research highlights contradictions between GDPR's privacy protections and marketers' reliance on granular data, yet identifies adaptive strategies like Next Best Action (NBA) frameworks for real-time consumer analytics and proposes consumer data marketplaces where users lease/sell data directly. By balancing compliance with agile solutions, GDPR emerges as a catalyst for ethical innovation, fostering long-term consumer trust and competitive parity in the EU's digital economy.

Adding to this, Bošković Batarelo, M. (2021) explored the impact of GDPR on digital marketing through a practical, risk-based methodology, using Data Protection Impact Assessments (DPIAs) to evaluate data processing risks and ensure compliance. The approach analyzed variables like consumer trust, privacy by design, and lawful processing grounds (e.g., legitimate interest or consent). A case study of Google Chrome's decision to block third-party cookies showed how companies are adopting Privacy-Enhancing Technologies (PETs), like differential privacy, to balance targeted advertising with user privacy. The research concluded that embedding privacy into marketing strategies not only strengthens consumer relationships but also reduces regulatory and reputational risks

In another study, Schweigert, V.-A., & Geyer-Schulz, A. (2019) explored the impact of the General Data Protection Regulation (GDPR) on marketing design and measurement through a practical case study using their in-house tracking system KIT Analytics. The research used an exploratory analysis of marketing activities for the Archives of Data Science journal, measuring user interactions without violating GDPR principles by replacing traditional tracking methods with pseudonym zed data collection. The findings demonstrated that integrating Permission Marketing (Godin, 1999) with GDPR-compliant

tools not only reduced legal risks but also improved customer trust and campaign effectiveness. The study suggests that respecting user consent and limiting data collection enhances marketing precision, reinforcing the value of privacy as a strategic advantage

Further reinforcing this, Kotch Obudho (2024) investigated the impact of data privacy laws on digital marketing through a desktop research methodology, analyzing global case studies to understand business adaptations to regulations like GDPR, CCPA, and LGPD. The research highlighted how companies like Tesco (UK) rebuilt their data practices to comply with GDPR, boosting consumer trust, with 74% of consumers feeling more secure post-compliance. In Brazil, Coca-Cola successfully balanced LGPD constraints with an engaging social media campaign, maintaining strong audience connections.
The study found that businesses investing in Privacy-Enhancing Technologies (PETs) gained long-term consumer loyalty, while those treating compliance as a formality saw minimal trust improvements. Ultimately, Obudho concluded that privacy laws, while costly, can become a strategic advantage for companies that prioritize ethical data practices and consumer education.

1.2 Platform adaptation on business model shifts

Digital platforms have faced significant challenges in aligning their business models with GDPR requirements. While some adaptations have enhanced user privacy, others have forced companies to rethink their monetization strategies. Shifting focus to platform adaptation, Mans, E. (2019) demonstrated through research on Facebook's profiling practices under the GDPR that while the platform adjusted its policies, it still struggles to fully comply with the regulation. Using a legal analysis approach, the study examined Facebook's data collection methods, consent mechanisms, and profiling techniques.
The results showed that although Facebook introduced more transparent privacy settings, the platform continued to rely on legitimate interest for advertising, which sometimes conflicted with GDPR requirements for valid consent. The study concluded that true GDPR compliance requires a deeper structural shift in how Facebook manages and monetizes personal data, beyond surface-level policy adjustments. (Mans, 2019*)*

Expanding on platform challenges, Böhmecke-Schwafert and Niebel (2023) conducted a case study analysis of Facebook's data-driven business model (DDBM) under the EU's General Data Protection Regulation (GDPR), employing Hartmann et al.'s (2016) taxonomy to evaluate five dimensions: data sources, key activities, offerings, target customers, and revenue streams. By analyzing Facebook's adaptation to GDPR's right to data portability such as enabling structured data exports (JSON/CSV) and discontinuing third-party data purchases—the study revealed that portability reduces monopolistic "lock-in" effects, allowing users to transfer data to competitors (e.g., Google+), while simultaneously spurring innovation by enabling startups to leverage exported data. However, GDPR's mandates risk diluting Facebook's ad-targeting precision (critical to its $40.7B ad revenue in 2017) and highlight contradictions between fostering competition and Facebook's enduring dominance via network effects. The findings underscore GDPR's dual role in challenging monopolistic practices and driving strategic shifts, such as Facebook's exploration of subscription models, to balance compliance with innovation. Key Terms: GDPR, Data Portability, DDBM, Lock-in Effect, Network Effects.

1.3 Advertising performance and revenue impact

The GDPR has had a tangible impact on digital advertising, with companies experiencing shifts in revenue and engagement metrics

Turning to advertising performance in a study by Wang, Jiang, and Yang (2023), the authors investigate the impact of GDPR compliance on display advertising performance, bid pricing, and revenue for a U.S.-based ad publisher with global reach. Focusing on 3.7 billion ad impressions from 6,000 creatives, the researchers employed a difference-in-differences (DID) methodology, comparing users with EU IP addresses (treatment group) against non-EU users (control group) before and after GDPR implementation. The results revealed that GDPR compliance led to moderate declines: a 2.1% drop in click-through rates, a 5.4% reduction in conversion rates, and a 5.7% decrease in revenue per click, driven by reduced advertiser bids and competition. Notably, the study highlighted industry-specific vulnerabilities: travel and financial services ads suffered the most, while retail and CPG ads were least affected. Crucially, the authors uncovered that contextual targeting placing ads on topic-relevant webpages (e.g., sports gear on athletic content) partially offset GDPR's negative effects, mitigating losses by up to 44%. However, brand image

(via contextual relevance) alone could not fully shield revenue, as indirect pathways like bid adjustments and advertiser attrition played roles. This suggests that while GDPR compliance challenges precision targeting, adaptive strategies leveraging webpage context offer a lifeline, balancing regulatory adherence with sustained ad efficacy.

In a similar vein, Wasteland's (2018) analysis of GDPR's impact on digital advertising revealed significant declines in behavioral targeting efficacy, particularly for centralized platforms like Google and Facebook, which suffered 22% drops in personalized ad revenue due to restrictions on cross-site tracking and automated profiling, while industries like travel and finance reliant on sensitive user data faced steeper losses (18–25%) compared to retail, which mitigated declines through contextual alignment (e.g., product ads on topic-relevant sites). The study emphasized decentralized data flows (e.g., block chain consent systems) and hybrid strategies blending first-party data with contextual signals to recover targeting precision, though challenges persisted in balancing innovation and compliance. Expanding on these findings,

Smith et al. (2024) noted modest post-GDPR declines in EU markets (5.7% revenue drop, 2.1% CTR fall) with travel and finance hardest hit (8.7% revenue loss), while retail and CPG thrived via contextual tactics (44% smaller declines for topic-aligned ads). Both studies underscored contextual targeting's compensatory role, stable advertiser ROI despite bid-price drops (-5.6%), and the viability of decentralized frameworks (e.g., federated learning, privacy-first IDs) to reconcile privacy compliance with market competitiveness, though fragmented regulations and consent fatigue remain hurdles. Together, they highlight GDPR's dual role as a disruptor and catalyst, urging industry adaptation through AI-driven contextual tools, niche content hubs, and harmonized regulatory standards to sustain growth in a privacy-centric landscape.

1.4 Compliance as a Strategic Lever for Trust and Risk Management

Beyond risk mitigation, GDPR compliance can serve as a strategic lever for organizations aiming to build consumer trust and strengthen governance ;The implementation of the General Data Protection Regulation (GDPR) in Croatia, enforced by the Croatian Personal Data Protection Agency (AZOP), marked a transformative alignment with EU standards, superseding prior frameworks such as constitutional privacy guarantees (Article 37),

The Personal Data Protection Act, and the 1981 Strasbourg Convention. GDPR's direct applicability introduced stringent requirements, including privacy by design, mandatory Data Protection Impact Assessments (DPIAs), and the appointment of Data Protection Officers (DPOs), with non-compliance penalties reaching up to 4% of global turnover. Atlantic Grupa d.d., a Zagreb-based multinational managing 5,500 employees and nearly one million personal data records, exemplified these challenges, adopting a structured compliance strategy involving comprehensive data inventory, risk assessment matrices to prioritize threats (e.g., IT system breaches), and mitigation measures like encryption, access restrictions, and updated policies. Governance efforts included DPO appointments, employee training, and cross-border data protocols, reducing risks from high (12) to medium-low (4). This case highlights the viability of proactive compliance through legal, technological, and organizational integration, offering a model for Croatian enterprises to navigate GDPR's demands while mitigating financial and reputational risk. (Krešimir Starčević, 2018)

Similarly, Barry, A. T. (2020) demonstrated through research on GDPR and local data laws in Guinea that telecom operators face unique challenges when complying with dual regulations. Using a regulatory compliance framework, the study analyzed the case of MTN Guinea, exploring variables like data security, employee training, and regulatory oversight. The findings indicated that while GDPR compliance improved data protection practices, it also exposed gaps in local infrastructure and legal clarity. Barry concluded that a hybrid approach, blending GDPR principles with tailored local policies, is necessary to achieve sustainable compliance.

Complementing this, DMA (2019) investigated the impact of GDPR on marketing practices using an industry survey-based methodology, collecting responses from marketing professionals and consumers. The research explored variables like consumer trust, compliance practices, and business performance. Findings showed a 34% increase in consumer trust, with brands like Unilever embedding legal experts in marketing teams, while eBay appointed privacy champions to ensure ongoing compliance. The study included case studies, such as The Guardian's GDPR campaign, which exceeded opt-in targets by 110%, and Google's €50 million fine for failing to meet transparency standards. Despite challenges, the DMA concluded that businesses viewing privacy as a competitive advantage experienced greater consumer loyalty and long-term brand strength

In a technical context, Çelebi, I. (2018) introduced Privacy Enhanced Secure Tropos (PESTOS), a privacy modeling language designed to help software engineers achieve GDPR compliance through a goal-actor-rule approach. The study used a meta-model analysis and validated the framework with identity and security experts to ensure correctness and usability. PESTOS mapped 21 technical GDPR articles into system goals, guiding engineers in selecting Privacy-Enhancing Technologies (PETs) and integrating Privacy by Design principles. A case study demonstrated how this approach helped organizations proactively meet regulatory requirements and reduce privacy risks, showing that structured modeling strengthens both compliance and system security.

1.5 GDPR's Broader Regulatory and Territorial Impact

Consumer awareness and expectations around data privacy have evolved in the wake of GDPR enforcement.

The research conducted by Heidi Ndilli-Ronkainen adopted a mixed-methods approach, combining qualitative and quantitative strategies to assess how subsidiaries of an international chemical company prepared their HR departments for GDPR compliance. Primary data was collected via structured questionnaires distributed to HR managers across nine EU/EEA subsidiaries, co-developed with the case company's HR supervisor to align with organizational needs, focusing on process identification, evaluation, and implementation phases. Secondary data from EU regulations, Finnish laws, and academic literature contextualized findings. Despite a 78% response rate (5 of 9 subsidiaries), limitations included self-reported bias and non-responses from some countries. A deductive analysis against the HR GDPR framework revealed most subsidiaries were unprepared for the 2018 enforcement deadline, with Lithuania progressing furthest and Germany fully compliant. Recommendations emphasized centralizing compliance efforts, appointing Data Protection Officers, and developing retention policies and training programs, highlighting gaps in documentation and governance. The study balanced academic rigor with practical insights, offering actionable steps while underscoring challenges in multinational regulatory adaptation.

In a legal context, De Terwangne, C. (2018) demonstrated through research on the GDPR's legal definitions and territorial scope that the regulation drastically expanded privacy protections beyond the EU. Using a doctrinal legal analysis, the study explored variables like data subject rights, processing limitations, and jurisdictional reach. The research revealed that the GDPR's broad definitions, such as "personal data" and "processing", created interpretive challenges for businesses, but also reinforced individual rights globally. De Terwangne concluded that the GDPR's extraterritorial effect set a new global privacy standard, influencing even non-EU jurisdictions.

Adding historical perspective, Daśko, N. (2016) explored the impact of the GDPR on European data protection laws, highlighting its transformative approach to consumer privacy through concepts like privacy by design, privacy by default, and data portability. Using a comparative legal analysis, the study examined the evolution of data protection from Directive 95/46/EC to the GDPR, analyzing case law like Google Spain to illustrate the regulation's broader territorial reach. The research emphasized that, while the GDPR enhances citizen rights and increases corporate accountability, it also presents compliance challenges, especially for smaller businesses. Ultimately, Daśko concluded that GDPR is not just a legal framework but a paradigm shift, balancing innovation with fundamental privacy rights

1.6 Consumer Perception, Behavior, and Privacy Empowerment

As businesses adapted internally, consumers themselves became more aware of their digital rights. The GDPR not only empowered users with greater control over their data but also influenced their interactions with brands.

Shifting to consumer behavior, Saerens, P. (2020) demonstrated through research on consumer knowledge of the GDPR and its impact on psychological responses to personalized online advertising that increased GDPR awareness reduces feelings of vulnerability and consumer reactance. Using a quantitative experimental approach, the study collected data via an online questionnaire where participants were shown a Facebook ad tailored to their recent searches. The research explored variables like privacy concerns, consumer empowerment, and psychological reactance. Results showed that participants

with greater GDPR knowledge felt less vulnerable but paradoxically had heightened privacy concerns. However, those same consumers exhibited lower reactance to personalized ads, confirming that privacy education mitigates negative ad responses. Saerens concluded that companies educating users about their privacy rights can decrease ad avoidance and foster better consumer-brand relationships.

Building on this, Balgobin, Y. (2018) demonstrated through a research on consumer control over personal data that privacy concerns and the adoption of Privacy-Enhancing Technologies (PETs) significantly shape consumer behavior and firm profitability. Using a mixed-methods approach, the research combined survey data from the ACSEL barometer and theoretical modeling to explore how privacy preferences influence willingness to share data, online purchases, and financial decisions.

With regard to the affective dimension of consumer privacy, the results showed that consumers using PETs were more willing to share personal information, as these tools restored trust in online services. For instance, the adoption of PETs increased consumers' likelihood of sharing data by 20%, demonstrating that control over privacy can enhance data availability rather than restrict it.

On the behavioral dimension of financial privacy, the research highlighted that consumers using non-bank payment instruments (like PayPal or Bitcoin) increased their online purchases while limiting the data exposed to banks. However, when privacy-enhancing behaviors were driven by distrust rather than proactive privacy management, banks faced more fragmented consumer data, impairing their risk assessment capabilities.

Ultimately, Balgobin concluded that privacy, far from being a barrier to data-driven business models, can be a strategic lever: firms that offer privacy-respecting services may build deeper consumer relationships and improve long-term data access, turning privacy compliance into a competitive advantage

Meanwhile, in Morocco, Bekkari Soukaina & Chakor Abdellatif (2022) demonstrated through their research on E-marketing and personal data protection that consumer consent and data security are central to modern marketing strategies. Using a regulatory analysis approach, the study examined the Moroccan CNDP law alongside the GDPR to explore how companies must balance innovation with legal compliance. The findings revealed that when consumers are granted explicit rights of access, rectification, and opposition, they are more likely to trust brands that transparently handle their personal data. The behavioral dimension showed that companies integrating privacy protection into their digital strategies

benefited from improved consumer retention. However, firms treating compliance as a constraint, without fostering consumer trust, struggled to maintain customer loyalty. Ultimately, the research concluded that data protection, rather than hindering marketing, can be leveraged as a competitive advantage when aligned with consumer expectations and legal obligations

Yet, the road to transparency was riddled with potholes.

Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle (2021) demonstrated through their research on "Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web" that since the enactment of the GDPR in 2018, there has been a significant increase in privacy awareness and policy adjustments across online services. Their findings indicate that while cookie banners and privacy notices have become more prevalent with an almost 40% increase in consent notices and a 60% growth in privacy policy volume compliance with GDPR standards remains inconsistent.

Regarding the transparency dimension, the study highlights that although websites disclose more information about data collection practices, many privacy policies still lack essential details, such as clear contact points for privacy inquiries or straightforward explanations of data rights. This aligns with earlier research on consumer privacy expectations, which showed that users prefer straightforward, accessible information when making privacy decisions.

On the behavioral dimension, the researchers observed that although more services provide options to opt out of data processing, users often face dark patterns intentionally complex interfaces designed to nudge them into accepting tracking cookies. Without a positive and user-friendly experience, the ability to opt out loses its effectiveness, similar to how loyalty to a brand's identity signs diminishes when the behavioral aspect of attitude lacks affective support in a rebranding context.

Ultimately, Kretschmer et al. concluded that, while the GDPR has undeniably pushed the web ecosystem towards more privacy-conscious practices, there is still room for improvement. They suggest that service providers follow stricter usability guidelines to align their practices not just with legal compliance but with user expectations, emphasizing that real privacy empowerment lies at the intersection of regulation, design simplicity, and user control

1.7 Ethical and Technological Evolution in Marketing and AI

Finally, privacy regulations have accelerated the ethical evolution of technology, especially in artificial intelligence and advanced analytics. As firms navigate the complexities of compliance, they are also laying the groundwork for a more responsible digital landscape.
As debates over AI ethics intensified, Tikkinen-Piri, Rohunen, and Markkula (2017) analyze the GDPR's transformative impact on personal data-intensive companies, contrasting its expanded scope and stricter mandates such as data minimization, accountability, and breach notifications with the 1995 Data Protection Directive (DIR95). The study identifies 12 key compliance aspects, including data protection by design, appointing a Data Protection Officer (DPO), ensuring data portability, and managing cross-border data transfers. The GDPR imposes significant operational burdens: companies must limit data collection to necessity, document processing activities, conduct impact assessments for high-risk operations, and implement mechanisms for user consent and right to erasure. Non-EU firms targeting EU users face extraterritorial compliance, while SMEs grapple with resource constraints and fines up to 4% of global revenue. Though the GDPR harmonizes EU data laws, challenges persist in interoperability standards, age verification for minors, and balancing transparency with agile business models. The framework underscores GDPR's dual role as a regulatory hurdle and a catalyst for trust-building through enhanced privacy practices.

In GDPR Impact on Computational Intelligence Research, Crockett, Goltz, and Garratt (2018) unravel the ethical labyrinth confronting computational intelligence (CI) in the wake of Europe's GDPR. The author's frame GDPR as a disruptor of opaque AI practices, mandating explain ability for automated decisions a stark challenge for neural networks and deep learning systems that operate as "black boxes." Through legal analysis of GDPR Articles 4 and 22 and case studies spanning self-driving cars, autonomous weapons, and deception detection systems like Silent Talker, the study exposes the tension between CI's complexity and GDPR's demand for transparency. For instance, AI-driven border control tools like iBorderCtrl must justify profiling decisions through interpretable logic, risking vulnerability to spoofing if explanations are overshared. The authors highlight GDPR's ripple effects: CI researchers now face Data Protection Impact Assessments (DPIAs) to evaluate risks, privacy-by-design integration, and ethical approvals processes that strain

international collaborations due to fragmented compliance frameworks. Their findings reveal industry-specific quandaries: while mortgage algorithms using decision trees can comply by outputting rules, neural networks in security contexts struggle to balance explain ability with operational secrecy. The narrative concludes with cautious optimism: GDPR compels a shift toward ethically aligned design (e.g., IEEE's guidelines), urging researchers to embed human oversight and transparency from inception. Yet, the path forward remains fraught, as CI's evolution risks outpacing regulatory clarity, leaving systems like autonomous weapons in ethical limbo. The study underscores that GDPR is not merely a legal hurdle but a catalyst for reimagining AI's role in society where innovation thrives only when anchored to accountability.

For smaller players, the GDPR era was a double-edged sword. Xuereb, K., Grima, S., Bezzina, F., Farrugia, A., & Marano, P. (2019) investigated the impact of GDPR on financial services in small European states using semi-structured interviews with 63 participants from different firms. The methodology combined quantitative analysis (MANOVA) and qualitative thematic analysis to explore variables like trust and reputation, training needs, and resource requirements. The results showed that while GDPR increased compliance costs and workload, it also strengthened consumer trust and institutional reputation. However, smaller states faced disproportionate burdens due to a one-size-fits-all regulatory approach, highlighting the need for more flexible compliance measures tailored to smaller economies

But the digital age's ethical dilemmas stretched beyond data.

Mathlouthi, E., Rana, A., & Rauf, S. (2024) demonstrated through research on GDPR's impact on SMEs in the European Union that while the regulation introduced compliance burdens, it also created

Competitive advantages for firms embracing transparency. Using a qualitative case study approach, the research explored variables like market entry barriers, compliance costs, and consumer trust. The findings showed that SMEs struggled with resource constraints, but those who invested in privacy-by-design practices gained market differentiation. Ultimately, the study concluded that GDPR, despite its challenges, could act as a regulatory tool to balance competition and consumer welfare.

As GDPR reshaped corporate accountability, the ethical spotlight expanded beyond institutions to individual actors in the digital sphere. Parallel to SMEs navigating

compliance burdens and AI systems grappling with transparency, influencers emerged as pivotal yet under regulated players in the data-driven marketplace.

Quettier, C. (2024) demonstrated through research on the ethical responsibilities of influencers in online product promotion that influencers hold significant power over young consumers' purchasing decisions. Using a qualitative exploratory approach, the study conducted 18 in-depth interviews with social media users, exploring variables like authenticity, transparency, and consumer vulnerability. The results indicated that influencers promoting products without disclosing sponsorships contribute to deceptive marketing practices, especially affecting younger, more impressionable audiences. The research concluded that reinforcing ethical guidelines and encouraging influencers to prioritize consumer well-being could mitigate harmful effects and restore trust in digital marketing.

Section 2: Conceptual Framework

2.1 SENSITIVE DATA

Sensitive data, legally termed "special categories of personal data" under the GDPR (Article 9), refers to information that, by its nature, poses heightened risks to an individual's privacy, dignity, or fundamental rights if misused, including data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric identifiers, health status, sexual orientation, or criminal history (European Parliament, 2016). Unlike general personal data, its processing is strictly prohibited unless justified by explicit consent, substantial public interest, or necessity for vital interests, with jurisdictions like the EU mandating enhanced safeguards (e.g., encryption, access controls) to mitigate risks .(ICO, 2023) Similarly, Algeria's Law 18-07 restricts processing such data without prior authorization from national regulators, reflecting global recognition of its uniquely invasive potential
(Law 18-07, Art. 33, 2018*).* This stringent framework contrasts with narrower definitions in laws like the U.S. HIPAA, which focuses primarily on health data, underscoring the GDPR's precautionary approach to balancing innovation and human rights. (Cohen, 2021)

2.2 Personal data:

Personal data is any information, in any form, that relates to an identified or identifiable natural person. This includes direct identifiers such as names, national identification numbers, or biometric markers (e.g., fingerprints), as well as indirect identifiers like IP addresses, geolocation data, vehicle license plates, or combinations of non-unique attributes (e.g., birthdate combined with postal code).

Under frameworks like the GDPR and Algeria's Law 18-07, identifiability hinges on whether the data can be linked to a person through "reasonable means," including contextual cross-referencing or emerging technologies. Notably, even pseudonymized data identifiers are masked but reversible remains classified as personal if re-identification is feasible.

The definition also extends to sensitive categories such as genetic, biometric, health, political, religious, or economic data, emphasizing the need for heightened protection. By

encompassing both explicit and inferred information, this broad scope acknowledges the evolving risks of modern data ecosystems, where fragmented datasets can coalesce into comprehensive personal profiles.

2.3 LEGAL FRAMWORK FOR DATA PROTECTION

Data protection refers to the legal and technical measures designed to safeguard personal information from unauthorized access, misuse, or disclosure. In an increasingly digitized world, where personal data drives innovation and economic growth, ensuring privacy has become a cornerstone of trust between individuals, businesses, and governments. Frameworks like the EU's General Data Protection Regulation (GDPR) and Algeria's Law 18-07 establish rules for collecting, processing, and storing data, emphasizing transparency, accountability, and individual rights. These regulations aim to balance technological progress with ethical responsibility, empowering individuals to control their data while holding organizations to higher standards of compliance. (ARADJI, G. n.d.)

- **Scope of Algeria's Personal Data Protection (Law 18/07)**

Algeria's personal data protection framework, primarily governed by Article 4 of the relevant legislation, applies to all forms of personal data processing, whether fully or partially automated or carried out manually. The law specifically targets data stored in or intended for manual filing systems, ensuring comprehensive coverage regardless of the technical method used. For the law to apply, three core conditions must be met. First, the data in question must qualify as "personal data" under Article 3, which excludes information related to legal entities such as company names, legal structures, or contact details. Second, the processing must involve operations like collection, storage, or consultation. Third, the entity handling the data can be any public or private organization, with no distinctions based on sector or purpose. By design, the law neutralizes potential loopholes tied to processing methods, ensuring uniform protection whether data is managed digitally or manually.
(ARADJI, G. n.d.)

- **Geographical Application**

The law's territorial scope extends to two key scenarios. The first applies to data controllers established in Algeria, defined as entities conducting effective activities on Algerian territory, regardless of their legal structure (e.g., local branches, subsidiaries, or offices). The second scenario covers foreign-based data controllers that process personal data using infrastructure or personnel located in Algeria, such as servers, local service providers, or representatives. In such cases, the Algerian representative or local service provider assumes responsibility for legal compliance, though the foreign controller remains jointly liable for any violations. This dual approach ensures accountability for both domestic and international actors operating within Algeria's jurisdiction. (ARADJI, G. n.d.)

- **Exceptions to the Law**

Articles 5 and 6 of the law outline specific exemptions to its application. These include purely personal or household activities, such as maintaining a private address book or contact list, which fall outside the law's regulatory scope. Additionally, low-risk processing activities those that do not involve profiling, cross-referencing sensitive data, or commercial exploitation are exempt. These exceptions aim to balance privacy protection with practical, everyday activities, ensuring the law does not unduly burden individuals or trivial operations. (ARADJI, G. n.d.)

- **Alignment with International Standards**

Algeria's framework reflects principles seen in global regulations like the EU's General Data Protection Regulation (GDPR), particularly in its emphasis on accountability for foreign entities using local resources and its focus on safeguarding individual freedoms. The law adopts a proportional approach, imposing rigorous protections for sensitive or high-risk data while allowing flexibility for harmless, routine practices. By harmonizing robust data security with pragmatic exemptions, Algeria's legislation seeks to foster trust in digital and manual systems alike, aligning with international norms without stifling innovation or personal autonomy. (ARADJI, G. n.d.)

- **Fundamental Principles of Personal Data Protection**

Algeria's Law 18-07 establishes core principles to govern the ethical and lawful handling of personal data, ensuring alignment with global privacy standards like the GDPR. These principles legality, fairness, purpose limitation, proportionality, and retention limits—form the backbone of data protection, mandating transparency, accountability, and respect for individual rights. By requiring organizations to process data only for justified purposes, minimize collection to what is strictly necessary, and retain information no longer than required, the law safeguards privacy while balancing operational needs. These principles not only guide compliance but also foster trust in a digital ecosystem increasingly reliant on responsible data stewardship. (ARADJI, G. n.d.)

- **Foundational Principles**

Algeria's Law 18-07 anchors personal data protection in four foundational principles that ensure ethical, transparent, and lawful handling of information. These principles legality and fairness, purpose limitation, proportionality, and retention limits act as pillars to balance organizational needs with individual rights. By mandating strict adherence to legal frameworks, precise objectives, minimal data collection, and time-bound storage, they create a robust system to prevent misuse and uphold privacy. Together, these principles foster accountability and trust, guiding organizations to align data practices with both legal obligations and societal expectations.

- **Legality and Fairness**

Under Article 9 of Algeria's Law 18-07, personal data must be processed lawfully and fairly. Lawfulness requires that data processing strictly complies with legal frameworks, such as obtaining explicit consent, fulfilling contractual obligations, or adhering to legal mandates. For example, a telecom company collecting customer data to comply with anti-fraud regulations acts lawfully. However, even lawful processing can be deemed unfair if it lacks transparency. Fairness demands clear communication about how data is used, ensuring no hidden agendas. A pre-ticked checkbox for marketing emails, for instance, violates fairness, as it assumes consent without active agreement. A process may be lawful

but unfair (e.g., using data for undisclosed third-party marketing) or fair but unlawful (e.g., transparently collecting data without a valid legal basis). Organizations must balance both principles to maintain trust and compliance.

- **Purpose Limitation**

The purpose limitation principle mandates that personal data be collected and processed only for specific, explicit, and legitimate purposes clearly communicated to the data subject. This prevents arbitrary repurposing of data. For example, a hospital collecting patient records for treatment cannot later use that data for pharmaceutical marketing without fresh consent. The purpose must be precise (e.g., "analyzing purchase history to recommend products") and documented in privacy policies. Vague objectives like "enhancing user experience" are insufficient. Article 9 also prohibits incompatible reuse: data collected for one purpose (e.g., processing credit card details for transactions) cannot be reused for unrelated activities (e.g., profiling spending habits) without renewed consent. This safeguards against mission creep, ensuring data is not exploited beyond its original intent.

- **Proportionality**

The proportionality principle requires that data collected be adequate, relevant, and non-excessive relative to the stated purpose. For instance, a job application portal requesting marital status for a software engineering role violates proportionality, as such details are irrelevant to technical skills. Proportionality also intersects with data accuracy: controllers must ensure information is exact, complete, and updated. A bank, for example, must verify customer addresses regularly to prevent errors. Inaccuracies (e.g., misspelled names) must be promptly rectified or deleted. This principle shifts accountability to organizations they must actively maintain data integrity, not merely deploy "best efforts." Failure risks operational inefficiencies (e.g., failed deliveries) and legal breaches.

- **Data Retention Limits**

Law 18-07 imposes strict data retention limits, requiring personal data to be stored only as

long as necessary to fulfill the declared purpose. For example, e-commerce platforms must delete payment details post-transaction unless legally mandated (e.g., tax records). Retention periods must be predefined (e.g., six months for customer service logs to resolve disputes). Exceptions exist for historical, statistical, or scientific purposes, but data must be anonymized. Post-retention, organizations must implement secure deletion or anonymization protocols. Indefinite storage "just in case" (e.g., retaining deactivated social media profiles) violates this principle unless data is anonymized.

2.3.1 Legal Bases for Data Processing

Under Algeria's Law 18-07, data processing must rest on a lawful foundation, ensuring personal information is handled ethically and transparently. These legal bases balance organizational needs with individual privacy rights, creating a framework for responsible data use. Below is an exploration of the primary legal grounds.

- **Consent**

Consent under Law 18-07 requires freely given, specific, informed, and unambiguous agreement (Article 3). Unlike passive acceptance (e.g., pre-ticked boxes), valid consent demands active opt-in mechanisms, such as unticked checkboxes. For example, a mobile app seeking location access must present a standalone requestnot bury it in terms of service? Article 32 mandates prior disclosure: individuals must be informed of the controller's identity, processing purposes, data recipients, and their rights (e.g., access, erasure). Consent is revocable at any time without penalty (Article 7). Organizations must document consent (e.g., timestamps, forms) for audit compliance. For minors, consent requires validation from a legal guardian, protecting under-16s from exploitative practices.

- **Exceptions to Consent**

Law 18-07 permits processing without consent under six lawful exceptions:

1. Legal Obligations (e.g., employers sharing employee data with social security agencies).
2. Contractual Necessity (e.g., processing delivery addresses for order fulfillment).
3. Public Interest (e.g., census data collection for urban planning).

4. Legitimate Interests (e.g., fraud prevention, provided they do not override individual rights).
5. Vital Interests (e.g., hospitals sharing patient data during emergencies).
6. Historical/Scientific Research (with anonymized data).

These exceptions balance organizational needs with privacy rights. For instance, a bank may process transaction data without consent for fraud detection (legitimate interest) but cannot use it for unsolicited marketing.

- **Documentation and Accountability**

Organizations must document consent and legal bases rigorously. For example, maintaining time stamped records of opt-ins or contracts justifying data processing. Controllers must also implement measures to protect consent records from tampering. During audits, failure to provide proof of lawful processing (e.g., consent forms, legal mandates) may result in penalties.

2.3.2 Rights of Individuals under Algeria's Law 18-07

The rights granted to individuals under Algeria's Law 18-07 are designed to ensure transparency, accountability, and control over personal data. These rights reflect the law's commitment to upholding human dignity, privacy, and public freedoms while preventing misuse of personal information. (ARADJI, G. n.d.)

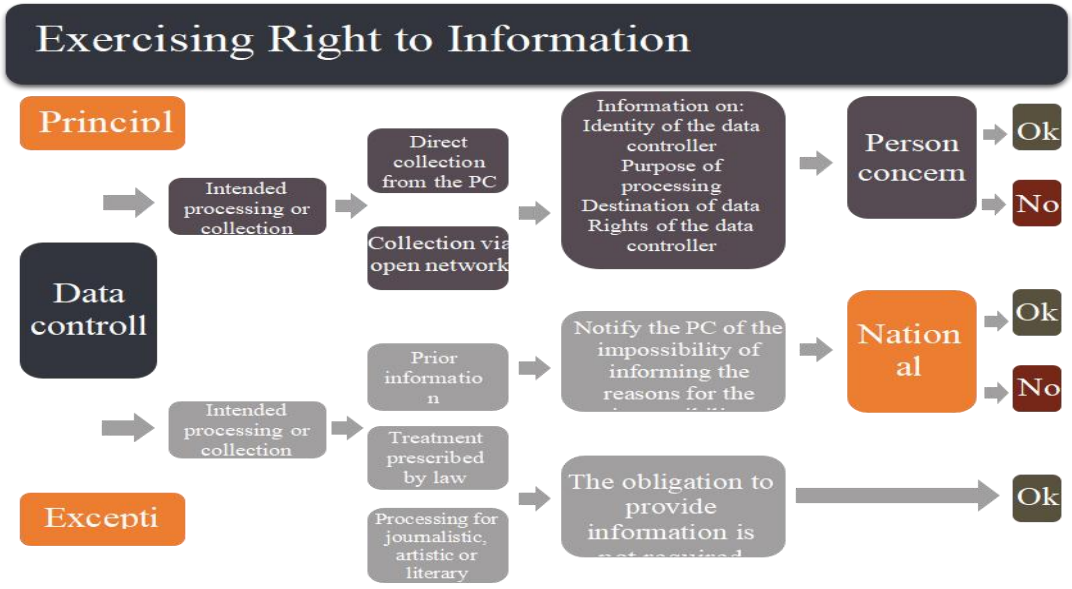
- **Right to Information (Article 32)**

Under Article 32, individuals have the right to know whether their personal data is being processed and to obtain clear, accessible details about the nature and purpose of such processing. This includes information about the identity of the data controller, the specific purposes of the processing, recipients of the data, and any international transfers.

For instance, a company using subcontractors to handle customer data must disclose the subcontractor's role and ensure individuals understand how their data is shared. The law mandates prior disclosure unless the individual already possesses this knowledge, such as in cases where data is collected from public sources like social media. However, exceptions apply when informing the individual is impossible such as in large-scale

historical or scientific research or when processing is legally mandated or for journalistic purposes. In such cases, the controller must notify the National Authority for Personal Data

Figure 1: *exercising right to information*

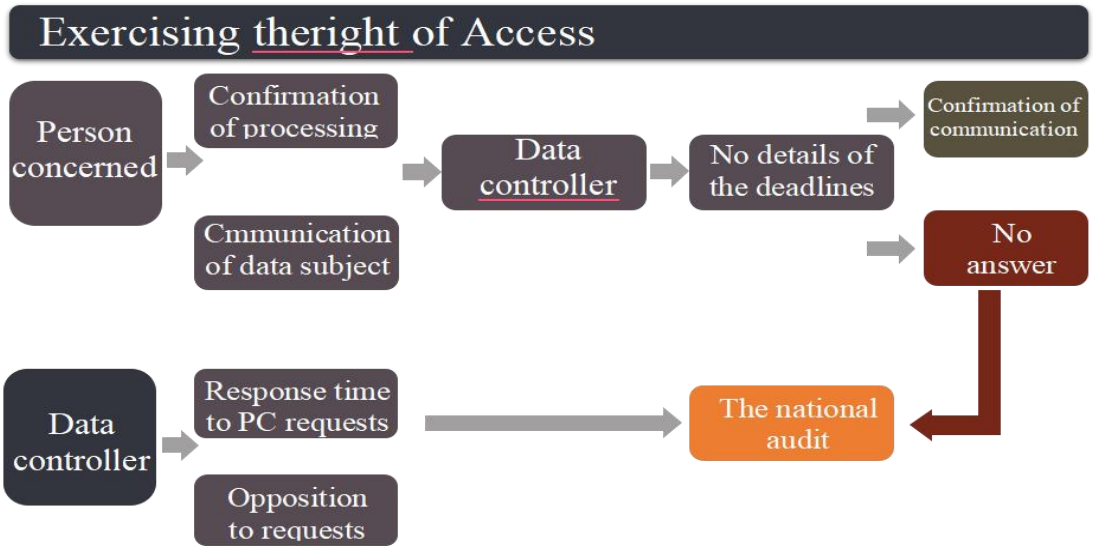


Protection (ANPDP) and justify the exemption

Source: (ARADJI, G. n.d.)

- **Right of Access (Article 34)**

Figure 2: exercising right of accesses



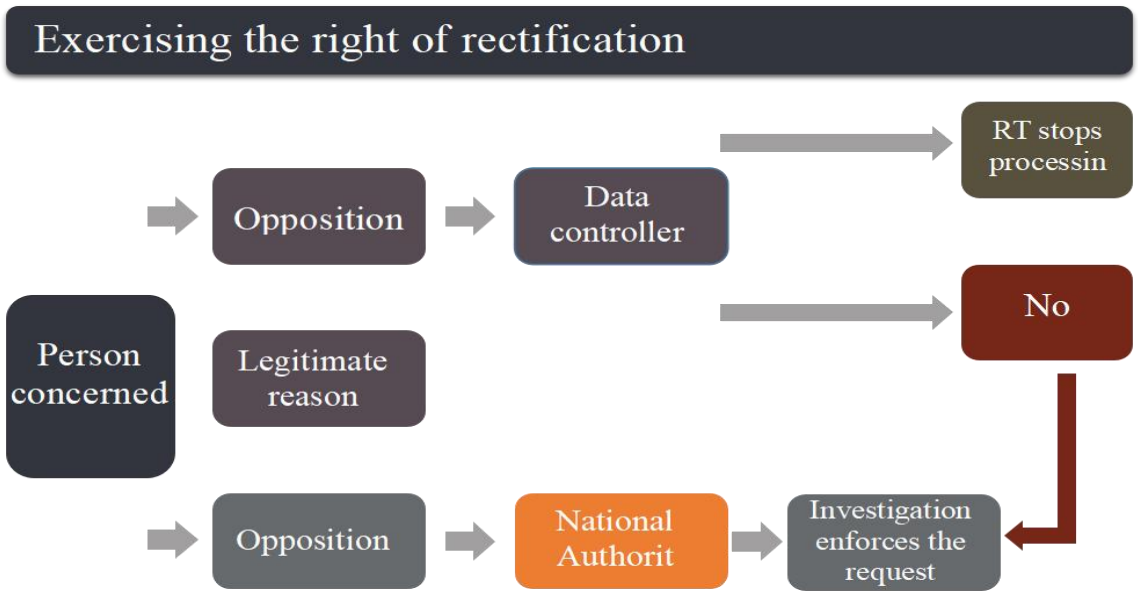
Source: (ARADJI, G. n.d.)

Article 34 grants individuals the right to access their personal data, including confirmation of whether it is being processed, the purposes of processing, and the categories of data involved. Controllers must provide a copy of the data in an intelligible format and disclose its origin if not collected directly from the individual.

For example, a patient may request access to their medical records to verify accuracy. Controllers may refuse manifestly abusive or repetitive requests but must prove the abuse to the ANPDP. Response times are prompt, though extensions may be granted for complex cases. This right ensures individuals can audit how their data is used and hold organizations accountable.

- **Right of Rectification (Article 35)**

***Figure 3**: exercising right of rectification*



Source: (ARADJI, G. n.d.)

Individuals may request corrections to inaccurate, incomplete, or unlawfully processed data under Article 35. Controllers must implement these changes free of charge within 10

days and notify third parties who received the data, such as marketing partners or financial institutions.

For instance, a bank must update a customer's outdated address and inform credit bureaus to prevent errors in credit reports. If the controller refuses or ignores the request, the individual may escalate the issue to the ANPDP, which investigates and enforces compliance. This right emphasizes the importance of data accuracy and accountability in maintaining trust.

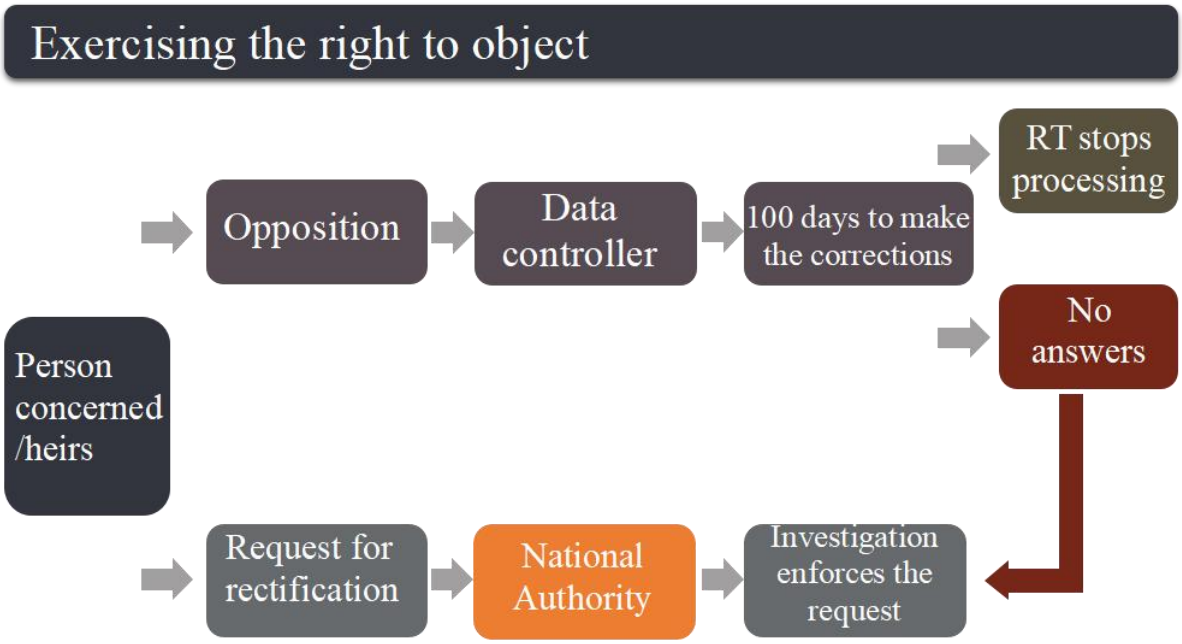
- **Right to Object (Article 36)**

Article 36 allows individuals to oppose data processing for legitimate reasons, particularly for commercial prospecting, such as unsolicited marketing emails or telemarketing.

To exercise this right, the individual must submit a written objection specifying the data and reasons for opposition. Controllers must cease processing unless they can demonstrate overriding legal or public interest grounds, such as tax audits or epidemiological studies.

For example, a consumer may opt out of a retailer's promotional campaigns while allowing the retailer to retain transaction records for warranty purposes. This right balances organizational needs with individual autonomy.

Figure 4: *exercising right to object*



Source: (ARADJI, G. n.d.)

2.3.3 Data Retention Limits (Article 9)

Personal data must not be retained longer than necessary to fulfill its declared purpose. Retention periods must align with the processing objective such as deleting customer payment details after order fulfillment unless extended for legal obligations like tax compliance. For historical, statistical, or scientific research, data must be anonymized to prevent re-identification. Organizations must implement secure deletion or anonymization protocols post-retention. Indefinite storage, such as retaining inactive social media profiles without justification, violates the law. This principle mitigates privacy risks and ensures data is not exploited beyond its original intent. (ARADJI, G. n.d.)

2.3.4 Subcontracting

Algeria's Law 18-07 establishes strict guidelines for subcontracting to ensure accountability and data protection, defining a subcontractor as any entity (e.g., IT firms, marketing agencies) that processes personal data on behalf of a data controller, per Article 3. The controller retains full responsibility for defining processing purposes and selecting subcontractors who provide sufficient technical and organizational safeguards, such as encryption or access controls, with certification requirements as potential proof of compliance. Subcontractors must act solely under the controller's instructions, adhering to confidentiality and security obligations, and cannot repurpose data for their own goals though they may become independent controllers if they process data autonomously. A binding contract, mandated by Article 39, formalizes this relationship, stipulating strict adherence to the controller's directives, data security protocols, and prohibitions against unauthorized use. This framework ensures subcontractors operate as accountable extensions of the controller, maintaining data integrity and aligning with the law's emphasis on transparency, security, and ethical data stewardship.
(ARADJI, G. n.d.)

2.3.5 Security and Confidentiality under Algeria's Law 18-07

Algeria's Law 18-07 mandates stringent security and confidentiality obligations for organizations handling personal data, requiring controllers to implement technical and organizational measures (e.g., encryption, access controls) tailored to mitigate risks such as data destruction, loss, alteration, or unauthorized access. These safeguards must align with the sensitivity of the data and evolving cyber threats, emphasizing proactive cybersecurity practices. Controllers must also notify the National Authority for Personal Data Protection (ANPDP) and affected individuals immediately in case of breaches compromising data confidentiality, integrity, or availability, unless pre-approved security measures sufficiently mitigate harm. Documentation of breaches, including remedial actions, is compulsory. Non-compliance risks severe penalties, including 3 years' imprisonment and fines up to 300,000 DZD (~$2,200), underscoring the law's focus on accountability. By integrating robust protections, breach transparency, and legal accountability, Law 18-07 fosters trust in Algeria's digital ecosystem while balancing innovation with ethical data stewardship. (Riad ARADJI, G. n.d.)

2.4 GENERAL DATA PROTECTION REGULATION (GDPR)

This chapter explores the General Data Protection Regulation (GDPR), the European Union's framework for safeguarding personal data. By the end of the chapter, you will grasp the regulation's core objectives, key definitions, and fundamental principles, as well as its significance in shaping modern data privacy standards. The content clarifies how the GDPR governs data processing, emphasizes accountability for organizations, and strengthens individual rights, providing a comprehensive understanding of this pivotal legislation.

- **Data Protection Directive (1995)**

The Data Protection Directive (DPD) of 1995 served as the foundational legislation safeguarding European citizens' rights regarding personal data *(Lynskey, 2015, p. 46).*

Originally influenced by guidelines from the Organization for Economic Co-operation and Development (OECD), the directive was formally adopted by the European Union as Directive 95/46/EC. (European Parliament and Council, 1995*)*

Its primary objectives included regulating the processing of personal data within EU member states, protecting EU citizens' privacy, and establishing rules for transferring data outside the EU to ensure comprehensive protection. The DPD aimed to harmonize data processing standards across member states; however, scholars such as Lynskey (2015, p. 47) argue that inconsistent interpretations of the directive by national governments and courts led to fragmented implementation. Despite these challenges, Lynskey emphasizes that key definitions and principles from the DPD were retained and expanded in the subsequent General Data Protection Regulation (GDPR).

- The DPD outlined six core principles governing data protection:

- Consent and transparency: Personal data must only be processed with the explicit consent of the data subject. (European Parliament and Council, 1995).

- Purpose limitation: Data collection must be limited to specific, legitimate objectives and not repurposed without additional consent (European Parliament and Council, 1995).

- Security safeguards: Controllers must implement technical and organizational measures to protect data against unauthorized access, alteration, or destruction (European Parliament and Council, 1995).
-
- Data subject rights: Individuals have the right to access, correct, or delete their data, as well as to inquire about the purposes and recipients of data processing (European Parliament and Council, 1995).

- Storage limitation: Data retention must not exceed the timeframe necessary for its original purpose. Exceptions apply only for historical, statistical, or archival purposes under Article 89(1) (European Parliament and Council, 1995).

While the DPD laid the groundwork for modern data privacy laws, its reliance on member states to transpose directives into national law resulted in uneven enforcement. For example, Lynskey (2015, p. 47) notes that ambiguities in the directive's language allowed varying legal interpretations, undermining its goal of harmonization. Nonetheless, the DPD's emphasis on accountability, consent, and cross-border data transfer rules directly influenced the GDPR's stricter, unified framework.

- **Introduction and Definition**

The General Data Protection Regulation (GDPR), enacted by the European Parliament and Council, functions as a legally binding framework to govern how organizations collect and process personal data of individuals within the European Union (EU). Unlike the earlier Data Protection Directive (DPD), which permitted member states to implement its guidelines through national laws, the GDPR standardizes data protection rules across all EU countries *(Gross, 2016, p. 1)*.

Both frameworks prioritize protecting EU citizens' rights—such as data confidentiality and control over personal information—but the GDPR imposes stricter accountability requirements and significant financial penalties for noncompliance. (Voigt & Bussche, 2017, p. 2; Lynskey, 2015, p. 46)

A critical distinction lies in the GDPR's expanded definition of personal data, which now encompasses any information capable of identifying an individual. This contrasts with the DPD, which allowed member states to interpret the term based on their national legal contexts. (Gross, 2016, p. 1)

Additionally, the GDPR operates as a direct regulation enforceable across the EU, whereas the DPD functioned as a directive requiring transposition into domestic law.

- Enforced on May 25, 2018, the GDPR outlines core principles for organizations, particularly in human resources (HR):

- Lawfulness and fairness: Data processing must be transparent and legally justified.

- Purpose limitation: Data collection is restricted to explicitly defined, legitimate purposes.

- Data minimization: Only necessary and relevant information may be collected.

- Accuracy: Organizations must ensure data remains current and error-free.

- Storage limitation: Data retention is permitted only for the duration required to fulfill its original purpose.

- Integrity and confidentiality: Robust technical measures are mandated to prevent unauthorized access, loss, or breaches.

  Cross-border transfers: Data may only be transferred outside the EU if the recipient jurisdiction ensures equivalent data protection standards. (Voigt & Bussche, 2017, p. 87)

  By unifying compliance obligations and emphasizing individual rights, the GDPR has redefined global standards for data privacy governance.

  The General Data Protection Regulation (GDPR) aims to impose binding requirements on companies that collect or process personal data of European citizens. This regulation introduces a series of obligations for organizations, starting with the appointment of a Data Controller

2.4.1 GDPR Obligations

According to Shulz and Hennis-Plasschaert (2016), the Data Controller is defined as: "The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data." The controller decides how the data will be used, how long it will be stored, and who will have access to it. Once appointed, the controller must adhere to specific rules to ensure GDPR compliance, as summarized by DigitalWallonia (2018).

The controller's responsibilities include:

1. Maintaining a Record of Processing Activities: This written log must include:

- The name and contact details of the Data Controller.
- The purposes of the data processing.
- A description of processing activities and categories of individuals affected.
- Any data transfers to non-EU countries.
- The data retention period.
- A general overview of security measures implemented.

However, companies with fewer than 250 employees are exempt from this requirement, except under certain conditions.

2. Conducting Risk Assessments: The controller must evaluate potential risks to individuals and implement strategies to mitigate those risks.

3. Implementing Protective Measures: Once risks are identified, the controller must establish technical and organizational measures to safeguard against potential threats.

4. Informing Data Subjects: The controller has a duty of transparency and must promptly inform individuals about the collection and use of their personal data.

5. Ensuring Data Accuracy: The controller must ensure the accuracy of the collected data and take steps to correct or delete inaccurate information.

6. Ensuring Data Security: Protecting data from unauthorized access, loss, or damage is essential. Security strategies should be based on the identified risks to maintain data authenticity, integrity, and confidentiality.

7. Managing Subprocessors: If the controller engages a third-party processor, they must ensure the processor provides adequate data protection guarantees.

8. Appointing a Data Protection Officer (DPO): The DPO advises the organization, trains staff handling personal data, and ensures GDPR compliance. The controller must provide the DPO with the necessary resources to carry out their duties effectively.

9. Enforcing Data Minimization: The controller must only collect and process data that is adequate, relevant, and limited to what is necessary for the intended purpose.

10. By following these obligations, organizations can better protect personal data, build trust with consumers, and avoid hefty penalties for non-compliance.

2.4.2 Individual Rights

The General Data Protection Regulation (GDPR) establishes a robust framework of enforceable rights, empowering individuals to actively manage their personal data within the EU/EEA. These rights, ranging from accessing and rectifying data to restricting its use or demanding erasure, are designed to ensure transparency, accountability, and user autonomy in an era of pervasive digital processing. By granting individuals tools to challenge unlawful practices, question automated decisions, and revoke consent, the GDPR shifts power dynamics between data subjects and organizations, prioritizing privacy as a fundamental freedom. This section dissects each right's scope, legal grounding, and real-world application, illustrating how they collectively safeguard dignity and agency in data-driven systems *(General Data Protection Regulation [GDPR], 2016)*

❖ Right to Access and Data Transparency (Article 15)

The Right to Access under the GDPR ensures individuals can obtain comprehensive insights into how their personal data is processed. Organizations are legally obligated to

confirm whether they hold an individual's data, disclose the purposes of processing, identify third parties with whom the data is shared, and specify retention periods. Additionally, individuals are entitled to receive a copy of their data in a structured, commonly used format. This right fosters transparency, enabling data subjects to verify compliance and challenge unlawful practices. For instance, a user may request a detailed breakdown of how a streaming service utilizes their viewing habits for algorithmic recommendations. This provision not only empowers individuals but also compels organizations to maintain meticulous records and justify data usage. (GDPR, European Data Protection Board [EDPB], 2021)

❖ Right to Accuracy and Rectification (Article 16)

The Right to Rectification mandates that individuals can request corrections to any inaccuracies or omissions in their personal data. Organizations must act promptly to amend records, ensuring data remains relevant, accurate, and fit for its intended purpose. This right is critical in contexts where erroneous data could harm an individual's financial standing, reputation, or legal rights. For example, correcting a misreported criminal record in a background check database ensures fair employment opportunities. The GDPR emphasizes that rectification is not merely a technical obligation but a safeguard against systemic biases and administrative errors (*GDPR, EDPB, 2020*).

❖ Right to Erasure and Digital Oblivion (Article 17)

The Right to Erasure, often termed the "Right to Be Forgotten," allows individuals to demand the deletion of their personal data under specific conditions. These include situations where data is no longer necessary for its original purpose, consent is withdrawn, or processing is deemed unlawful. However, exceptions exist for legal compliance (e.g., tax records) or public interest (e.g., crime prevention). A landmark case, Google LLC v. CNIL (2019), clarified the global scope of this right, requiring search engines to delist outdated or irrelevant information upon request. This right empowers individuals to control their digital footprint, such as deleting abandoned social media profiles. (CNIL, 2019)

❖ Right to Processing Restriction and Data Integrity (Article 18)

Individuals may invoke the Right to Restrict Processing to temporarily halt the use of their data while allowing organizations to retain it. This applies when data accuracy is contested, processing is unlawful, or the individual opposes erasure despite the organization claiming legitimate interests. For example, a patient disputing the accuracy of a medical diagnosis may block a clinic from sharing their records until the issue is resolved. This right balances organizational needs with individual autonomy, ensuring data integrity without permanent deletion. (EDPB, 2022)

❖ Right to Data Portability and Interoperability (Article 20)

The Right to Data Portability enables individuals to obtain and transfer their data between service providers in a machine-readable format (e.g., JSON, XML). This promotes market competition and user autonomy, particularly in sectors like finance, telecommunications, and cloud services. For instance, a customer switching banks can seamlessly migrate transaction histories to a new provider. The EDPB's 2023 guidelines emphasize that organizations must avoid technical barriers, ensuring data is structured in open formats to facilitate interoperability. (EDPB, 2023*)*

❖ Right to Object and Opt-Out Mechanisms (Article 21)

The Right to Object permits individuals to oppose data processing for reasons specific to their situation, including direct marketing, profiling, or processing based on public interest. Organizations must cease processing unless they demonstrate compelling legitimate grounds that override the individual's rights. For example, a retail chain using purchase history for targeted ads must honor a customer's opt-out request. This right is pivotal in curbing intrusive practices, such as AI-driven behavioral tracking. (Wachter et al., 2021)

❖ Right to Human Intervention in Algorithmic Decisions (Article 22)

This right protects individuals from decisions made solely by automated systems (e.g., AI, algorithms) that significantly affect their legal rights, financial status, or personal well-being. Data subjects may demand human intervention, contest decisions, or request explanations. For example, a loan applicant rejected by an AI system can appeal for a manual review. Scholars like Selbst and Powles (2018) argue this provision is essential to prevent opaque, biased outcomes in automated decision-making.

Organizations must proactively provide clear, accessible information about data processing activities, including purposes, legal bases, retention periods, and rights. This information must be communicated in plain language, free of charge, and without undue delay. For example, a fitness app must explain how it uses heart rate data for health insights during onboarding. The UK's Information Commissioner's Office (2023) emphasizes that vague or overly technical privacy policies violate this right. (Information Commissioner's Office [ICO], 2023)

❖ ***Right to Third-Party Notification (Article 19)***

If data is rectified, erased, or restricted, organizations must notify all third parties with whom the data was shared, unless impractical. For example, a university correcting a student's academic record must inform scholarship providers or employers who previously accessed the data. This ensures consistency and prevents outdated information from influencing decisions. (EDPB, 2021)

❖ **Right to Consent Revocation and User Autonomy (Article 7)**

Individuals may withdraw consent for data processing at any time, as easily as it was granted. Withdrawal does not affect the legality of prior processing. For instance, a user revoking consent for location tracking on a navigation app must be able to do so via a single click. Legal scholars like Zarsky (2024) highlight this right as foundational for maintaining trust in digital ecosystems.

2.5 Compliance:

Refers to the adherence to applicable rules and standards governing economic activities. This encompasses national, European, and international regulations across diverse domains such as data protection (GDPR compliance, law (18/07)), workplace health and safety, environmental protection, taxation, competition law, fair trade, and more. The goal of compliance is to promote and demonstrate transparent, ethical, and lawful business practices while safeguarding customers and employees. Compliance has become a critical priority for modern enterprises, as consumer expectations for corporate accountability continue to rise globally. Failures in compliance are increasingly scrutinized and publicly exposed, underscoring the need for organizations to rigorously align their operations with legal and ethical frameworks. (Lefebvre Dalloz, 2025)

2.5.2 Regulatory Risks of Non-Compliance

Beyond ethical and transparency concerns, failure to comply with regulatory requirements exposes organizations to significant risks: penalties, fines, legal actions, reputational damage, harm to brand image, employee attrition, and more. Compliance policies involve all stakeholders within a company. In cases of non-compliance, individuals may face sanctions proportionate to their level of responsibility. (Lefebvre Dalloz, 2025)

2.5.3How data protection builds customer trust and loyalty

As global data privacy regulations advance, public consciousness around digital rights grows in tandem. The 2018 introduction of the GDPR marked a pivotal shift in accountability standards, redefining consumer expectations that continue to influence business practices today. Beyond legal mandates, robust data protection has emerged as a critical foundation for fostering customer trust and loyalty a strategic asset in an era where privacy breaches can irreparably damage reputations.

The *2024 Data Privacy Benchmark Study* underscores this urgency: 94% of businesses report that customers would abandon their services if data protection measures failed.

2.6Customer loyalty:

2.6.1 Definition:

Customer loyalty has been defined in various ways in the marketing literature. According to Barbaray (2016), "customer loyalty is the result of a favorable attitude of an individual towards a brand (a product or a service) that results in repeated purchases".

Similarly, Jacoby and Keyner (as cited in Vio, 2006) describe brand loyalty as "the biased [non-random] response expressed in terms of purchase behavior over time by a decision-making unit towards one or more brands selected among a set of comparable brands, and it is the result of a psychological process (decision-making and evaluation)" .

Trinquecoste (n.d.) explains loyalty more simply, stating that it "can be expressed through consumption behaviors and explained by favorable consumer attitudes towards products or brands".

Finally, Kotler, Keller, and Manceau (2012) define loyalty as "a deep commitment to

Repurchase or re-patronize a preferred product or service consistently in the future despite situational influences and marketing efforts having the potential to cause switching behavior" (p. 158).

These various perspectives highlight that customer loyalty is not just behavioral but also rooted in psychological commitment and positive attitudes toward a brand.

2.6.2 Types of Loyalty

According to Lendrevie, Lévy, and Baynast (2015), loyalty can take several forms:

- **Absolute Loyalty and Relative Loyalty**

Absolute loyalty, meaning exclusive loyalty, is typically observed in businesses that sell their services through subscriptions (for example, telecommunications companies). In this case, a customer is considered loyal only if they renew their subscription at the end of the

term; otherwise, they are seen as disloyal.
Relative loyalty, on the other hand, refers to customers who make the majority, or at least a significant portion, of their purchases in a specific product or service category from a particular company.

❖ **Objective Loyalty and Subjective Loyalty**

Loyalty can also be classified as objective or subjective.
Objective loyalty is based on actual behaviors, such as repeat purchases.
Subjective loyalty, however, refers to mental attitudes like feelings of attachment, closeness, or preference, which are typically measured through surveys.
Marketing managers often focus on objective loyalty, emphasizing what the consumer actually does rather than what they think or say. Nevertheless, to evaluate the strength of loyalty and to predict future behavior, subjective loyalty measures are also taken seriously into account.

Like any attitude, loyalty consists of three main components that can be measured through surveys:

- **Cognitive component**: the consumer's preference for a brand or company.
- **Affective component**: feelings of emotional attachment or closeness to the brand.
- **Conative component**: the consumer's intention to repurchase.

2.6.3 Approaches to Loyalty

When it comes to customer loyalty, two major approaches can be distinguished: the behaviorist (behavioral) approach and the cognitive (attitudinal) approach (Lehu, 2003).

❖ ***The Behaviorist Approach***

As its name suggests, the behaviorist approach to brand loyalty is based on the observation of consumer behavior. Loyalty is seen as a sequence of repeated purchases in favor of the same brand. However, this approach has an inherent limitation: the uncertainty of future consumer behavior, meaning that purchasing patterns can change over time.

Within this framework, consumer loyalty can be classified into several types:

- **Conversion**: absolute loyalty to a specific brand.
- **Experimentation**: systematically testing different commercial offers.

- **Transition**: gradually shifting allegiance from one brand to another.
- **Mixed Loyalty**: alternating consumption among various brands.

❖ ***The Cognitive Approach***

The cognitive approach offers a richer understanding by introducing attitudes as key explanatory factors of loyalty. According to this perspective, a consumer will only be loyal to a brand if they have first developed a positive attitude toward it. Therefore, attitude formation precedes the actual behavior.

This approach is particularly relevant in situations involving high consumer involvement, where individuals exhibit a strong need for cognition. This distinction plays a crucial role in designing loyalty strategies. For consumers with a low need for cognition, it is preferable to focus on product placement and shelf visibility, encouraging comparison among brands. In contrast, for consumers with a high need for cognition, investing in advertising communication becomes more effective. However, advertising strategies must be carefully designed and pre-tested to ensure their relevance and impact.

Thus, concepts such as perceived risk, involvement, reference groups, and decision-making processes are critical to understanding and building consumer loyalty.

2.6.3 Passive Loyalty and Active Loyalty

When considering both the behavioral and attitudinal aspects of loyalty simultaneously, two levels of loyalty can be distinguished: passive loyalty and active loyalty.(Lendrevie, Lévy, & Baynast, 2015)

❖ **Passive Loyalty:**

Passive loyalty arises from personal factors (such as routine habits or the perceived risks of switching brands) or external constraints that make it difficult, or even impossible, for a customer to change brands. It can also result from inertia, laziness, or circumstances such as the unavailability of competing products. Moreover, passive loyalty may stem from perceived risk the fear that switching brands or suppliers might lead to a worse outcome.

The extreme form of passive loyalty is forced loyalty, where the customer remains loyal simply because they have no choice. Examples include local monopolies, or suppliers who lock customers in through long-term contracts, contracts that can only be canceled during specific periods, or by imposing high switching costs.
This type of loyalty is considered fragile because it can quickly disappear if there are changes in the legal, economic, or commercial environment (Lendrevie et al., 2015).

- **Active Loyalty:**
  Active loyalty, on the other hand, is the result of a customer's rational or emotional attachment or preference for a particular brand or supplier. This form of loyalty is stronger and more durable than passive loyalty, as it is more resistant to unfavorable changes in the surrounding environment. (Lendrevie et al., 2015).

2.7CUSTOMER LOYALTY DRIVERS

2.7.1 CUSTOMER TRUST

2.7.1.1 Definition of Customer Trust

Customer trust is a critical element that drives loyalty and enhances business success. Trust is defined as the belief that a company will consistently meet the customer's expectations through transparent, dependable, and honest behavior. Building and maintaining trust requires companies to not only meet their promises but also engage in emotionally resonant interactions with customers that foster long-term relationships. (Bishop, 2023)

2.7.1.2 The Age of the Customer

The "Age of the Customer" emerged in the early 2010s, when consumers became more connected than ever before. The increasing access to information and resources significantly raised customer expectations. According to Gartner (2023), 74% of customers now demand more from brands—not only in terms of products and services but also in how they are treated. In this context, customer trust has become even more integral to business success.

The Impact of Trust on Customer Loyalty

Building customer trust is crucial for enhancing customer loyalty. Research indicates that trust plays a pivotal role in shaping consumer loyalty and future behavior. A study by Gartner (2023) highlights that 83% of consumers would avoid doing business with

companies they do not trust. Emotional connections, characterized by dependability and transparency, have a greater influence on consumer behavior than purely cognitive evaluations of the brand. Trust is therefore an essential driver of long-term loyalty and positive business outcomes.

2.7.1.3 Strategies for Building Customer Trust

To establish and nurture trust, companies must focus on the following strategies: prioritizing customer service, promoting authenticity and transparency, responding to customer feedback, engaging meaningfully with customers, investing in employee training, and tracking metrics that align with trust-building efforts. These strategies help create a trust-based relationship that enhances customer satisfaction and drives loyalty (Bishop, 2023).

2.7.2 Satisfaction

2.7.2.1 Definition of Satisfaction:

Satisfaction is a central concept in consumer psychology and marketing behavior. According to several researchers, satisfaction can be defined as "the feeling of pleasure or displeasure that results from comparing prior expectations with actual consumption experience" (Lendrevie, Lévy, & Baynast, 2015).

Kotler, Keller, and Manceau (2015) similarly define satisfaction as "the positive or negative impression felt by a customer following a purchasing and/or consumption experience. It results from a comparison between the customer's expectations regarding a product and the perceived performance of that product". In the same vein, Llossa (as cited in Barbaray, 2015) describes satisfaction as "based on a comparison between the perceived performance of a service and a pre-established standard".

From these definitions, it can be concluded that satisfaction reflects the emotional reaction experienced by a customer after the consumption of a good or service. This emotional state can be positive, indicating that the consumer has received what they desired from the consumption experience, or negative, implying that the consumer’s expectations were not met. Subsequently, the customer will express satisfaction or dissatisfaction through their reactions and purchasing behavior.

2.7.2.2 Modes of Satisfaction

Customer satisfaction manifests in various modes depending on the situational context (Vanhamme, 2005):

- *Satisfaction as Pleasure*

  Occurs when a product/service induces happiness (e.g., listening to music). This state resembles positive reinforcement, involving active processing of expectations, performance, non-confirmation, and attribution. It includes moderate-to-high levels of activation, interest, and joy-related emotions.

- *Satisfaction as Relief:*
  - Arises when a product/service eliminates an aversive state (e.g., aspirin for headaches).
  - Requires active cognitive processing of expectations, performance, non-confirmation, and attribution.
  - Involves higher activation and interest compared to other modes).

- *Satisfaction as Admiration:*

  Characterized by respect and admiration for a product/service (e.g., high-tech products)

- *Satisfaction as Trust:*

  Defined by confidence in a product/service's reliability (e.g., dependence on a dishwasher for someone who dislikes washing dishes)

- *Satisfaction as Helplessness:*

  Marked by negative dependency on a product/service (e.g., inability to function without a car, even briefly).

- *Satisfaction as Resignation:*

  Involves passive acceptance (e.g., acknowledging that a newly purchased computer will soon become obsolete).

- *Satisfaction as Love:*

  Represents an emotional, behavioral, and psychological bond with a product/service (e.g., identifying with a brand). This is the deepest mode of satisfaction.

- *Dissatisfaction as Disappointment*:

  Combines surprise with negative emotions like sadness (e.g., unavailability of a desired product/service)

- *Dissatisfaction as Indignation:*

  Blends surprise and anger (e.g., retrieving a car from a mechanic with stained seats)

- *Dissatisfaction as Disorientation*:

  Characterized by disbelief at an unexpected outcome (e.g., finding a foreign object in a product, like a tomato in laundry detergent).

- *Dissatisfaction as Alert*

  Involves anxiety or fear about using a product (e.g., concerns about safety features) .

CHAPTER II: METHODOLOGICAL CONTEXT FRAMEWORK AND ORGANISATIONAL

Section 1: Methodological framework

1.1 Epistemological Posture:

This research adopts a positivist epistemological posture, grounded in a hypothetico-deductive reasoning framework. This approach is particularly appropriate for studying the impact of data protection laws (such as the GDPR and Algeria's Law 18/07) on customer loyalty, by testing a set of predetermined hypotheses derived from existing theories. Positivism is founded on the belief that reality is objective and can be measured and understood through observable phenomena (Gavard-Perret et al., 2012). In this view, knowledge is acquired by formulating hypotheses and verifying them against empirical data in a systematic and unbiased manner (Dudovskiy, n.d.). This methodology allows for the identification of causal relationships and is thus suitable for understanding how compliance with data protection regulations influences customer trust and satisfaction, which in turn affect loyalty. By maintaining axiological neutrality and relying on quantifiable data collected from structured questionnaires, the study ensures a high degree of objectivity and replicability. Such an approach is ideal for assessing the mediating role of psychological variables like trust and satisfaction in the relationship between regulatory compliance and consumer behavior (University of Geneva, n.d.).

1.2 Methodological Approach

The main objective of this research is to assess the impact of compliance with data protection laws (such as the GDPR and Algeria's Law 18/07) on customer loyalty, while examining the mediating roles of trust and satisfaction. To evaluate this cause-and-effect relationship, we apply quantitative statistical methods aimed at measuring the influence of a specific legal compliance intervention (the independent variable) on psychological and behavioral outcomes (the dependent variables). The central aim is to determine whether adherence to data protection regulations leads to changes in trust, satisfaction, and ultimately loyalty, and to what extent these variables are interrelated. Consequently, we adopted a quantitative experimental approach, operationalized through a structured survey administered to a representative sample of the target population. This methodological choice aligns with our positivist epistemological posture, relying on a hypothetico-deductive reasoning process to verify our proposed hypotheses through empirical data analysis.

1.3 Methods and Instruments of Data Collection

1.3.1 Measurement Instrument

To assess and quantify the relationships among the core variables of this research, a structured questionnaire was administered. This tool allows for the systematic measurement of respondents' perceptions regarding compliance with data protection laws and its anticipated impact on customer trust, satisfaction, and ultimately, customer loyalty.

1.3.2 Questionnaire Design

The questionnaire serves as the principal instrument for data collection. It consists of a series of logically ordered questions intended to elicit participants' opinions, perceptions, and evaluations. It was specifically designed to examine the theoretical relationships defined in our conceptual framework, namely: perceived compliance with data protection laws, customer trust, customer satisfaction, and customer loyalty.

The questionnaire is divided into six main sections:

- **Introduction and Informed Consent**: This section briefly presents the study's purpose and seeks the participants' informed consent.
- **Demographic Information**: Collects sociodemographic data such as age, gender, and length of relationship with the company to define the respondent profile.
-
- **Perceived Data Protection Compliance**: This section evaluates respondents' perceptions of the company's adherence to data protection regulations (such as GDPR or Algeria's Law 18/07).
- **Customer Trust**: Measures customers' perceptions of the company's reliability, honesty, and ability to safeguard personal data.
- **Customer Satisfaction**: Captures the respondents' overall evaluation of their experiences with the company, including the fulfillment of expectations and general contentment.
- **Customer Loyalty**: Assesses behavioral intentions such as repurchase, preference, and willingness to recommend the brand to others.

Measurement Scale

All questionnaire items were adapted from validated scales in the marketing and consumer behavior literature. Each construct is measured using a five-point Likert scale, ranging from “Strongly disagree” (1) to “Strongly agree” (5). These scales offer a nuanced assessment of the degree of agreement or disagreement with the statements related to the study variables.

The items used to measure the constructs of **perceived compliance**, **trust**, **satisfaction**, and **loyalty** were drawn from established studies), and are summarized in the table that follows:

Table 2: Table of measurement items

Variables	Items
Compliance	I believe this company intends to comply with data protection laws (Law 18/07). This company is likely to handle my personal data in accordance with legal requirements. I expect this company to respect my privacy rights in the future. I believe the company will be transparent about how it uses my personal data. This company seems committed to protecting customer data according to regulations.
Trust	I feel confident that this company will keep my personal data secure. I believe this company can be trusted to act in my best interest regarding data usage. I trust this company to handle my personal information responsibly. I would feel safe sharing personal data with this company in the future.
	I would be satisfied if this company complies with data protection laws.

Satisfaction	Knowing the company respects data privacy would increase my satisfaction. I feel that compliance with privacy laws is important to my satisfaction with the service. The company's efforts in protecting my data would make me feel valued.
Loyalty	I am likely to remain a customer of this company if it complies with data protection laws. I would recommend this company to others if it demonstrates commitment to data protection. If the company protects my personal data well, I would continue using its services. I would prefer this company over others because it respects customer data privacy.

Source: Developed by ourselves

1.4 Sample and Survey Implementation:

1.4.1 Study population:

The study population consists of individuals who have had direct interactions with the physical branch of the SAA agency. Specifically, these are current or potential customers who have visited the agency to access its services. This group represents a relevant and informed sample, as they have been exposed to the company's data management practices, allowing for an accurate assessment of their perceptions in terms of trust, satisfaction, and loyalty. To ensure the validity of the research, participants are required to meet a specific eligibility criterion: having engaged with the agency's services at least once. This ensures that respondents have firsthand experience, enabling a focused and meaningful analysis of their attitudes and behaviors in the context of a prospective compliance with Law 18/07 on personal data protection.

1.4.2 Sampling method:

The target population of this study consists of individuals covered by SAA's (Société Algérienne d'Assurance) car insurance services, including both existing and prospective clients who engage with the agency. However, due to confidentiality considerations, the precise number of individuals within this population remains undisclosed. As a result, the sample size was calculated using a standard method suited for populations of unknown size, ensuring both the reliability of the results and the representativeness of the sample.

$$\boldsymbol{n0 = \frac{Z^2 \times p \times (1 - p)}{e^2}}$$

Cochran's Formula

Where:

n: refers to the sample size

Z: represents the Z-score, which is determined by the confidence level selected by the researcher.

The Z-score: signifies how many standard deviations a raw score or data point is from the mean. For a confidence level of 95%, which is typically used in human population studies, the Z-score is 1.96.

P: is the estimated proportion of a specific attribute present in the population.

Essentially, it's the anticipated percentage of the population that possesses the desired attribute. It can also be expressed as the standard deviation. A proportion of

0.5 is usually used in human population studies.

e: stands for the margin of error or confidence interval

This is the acceptable error margin in selecting our sample. The margin of error typically ranges from 1% to 10% in human population studies. In this case, it's considered as 5%.

By applying this Cochran's Formula, we get:

$$\boldsymbol{n}0 = \frac{1{,}96^2 \cdot 0{,}5 \cdot (1 - 0{,}5)}{0{,}05^2} = 384 + 10\% = 422$$

1.4.3 Practical Modalities of the Survey

Mode of Administration:

The questionnaire was administered physically at the central agency of SAA in Bab Ezzouar, using a digital tablet to facilitate participants' responses on-site. This method allowed for direct interaction with individuals who have experience with the company's services, ensuring the relevance and reliability of the responses collected.

The questionnaire was validated by the academic supervisor and the SAA agency representatives as part of the internship project, ensuring its alignment with the research objectives.

1.4.3.1 Survey Period

The data collection process was conducted during the internship period at the SAA central agency. The survey was carried out between April 5 and 25, 2025, allowing sufficient time to collect responses from physical visitors using a digital tablet.

1.4.3.2 Data Processing and Analysis Method

The collected data were analyzed using IBM SPSS Statistics (version 27.0) for statistical analysis. The analytical procedure followed these steps, and structural equation modeling (SEM) was conducted using AMOS."

- **Step 1: Data Cleaning and Preparation**

- The collected responses were imported into IBM SPSS for initial treatment, including variable coding and formatting.
- The dataset was examined for missing values, extreme outliers, and inconsistencies to ensure data reliability.
- Tests for multicollinearity and normality were performed to assess the adequacy of the dataset for further analysis.

Step 2: Descriptive Analysis

A descriptive statistical analysis was conducted to outline the profile of the respondents and summarize the key characteristics of the sample.

- Frequencies and percentages were calculated to describe socio-demographic variables such as age, gender, and duration of the relationship with the company.
- Graphical representations (bar charts and histograms) were used to visualize the distribution of responses across each item, along with their respective mean scores, to provide a comprehensive overview of the participants' evaluations.

Step 3: Confirmatory Factor Analysis (CFA)

This phase focused on verifying the robustness and consistency of the measurement model, based on the following objectives:

- To assess the structure and dimensionality of the constructs.
- To evaluate the internal consistency, convergent validity, and discriminant validity of the variables measured.
- To refine the model by identifying and removing items that did not load significantly on their expected factors.

Step 4: Hypotheses Testing

The hypotheses were tested using statistical techniques available in IBM SPSS Statistics (version 2025). Specifically, multiple linear regression analysis was employed to examine the relationships between the independent, mediating, and dependent variables. This approach allowed for the assessment of direct effects and initial support for the proposed relationships. To further analyze mediation effects and validate the structural relationships

within the conceptual model, Structural Equation Modeling (SEM) was conducted using AMOS. This enabled the examination of both direct and indirect pathways, providing a comprehensive empirical validation of the proposed hypotheses.

Section 2: Organizational Context

2.1 Saa's Assurances presentation:

The (Société Nationale d'Assurance) SAA is a leading public economic enterprise in Algeria, authorized to operate across all insurance and reinsurance branches. Established in 1963, SAA is the country's first insurance company and has since built a strong legacy based on expertise, responsibility, leadership, and commitment.

With over 3,000 employees and a network of more than 520 sales offices nationwide, SAA offers a wide range of products tailored to individuals, professionals, institutions, and public entities.

Over the decades, SAA has undergone major strategic transformations, including capital increases (up to 35 billion DZD in recent years), diversification of its portfolio, and solid financial performance, making it a resilient market leader. Today, SAA continues to play a pivotal role in the development of Algeria's insurance sector while maintaining trust-based relationships with its clients and partners.

2.2 SAA Services

The (Société Nationale d'Assurance) (SAA) provides comprehensive insurance and reinsurance solutions for individuals, businesses, and public institutions. Its services are organized into five main categories:

1. **Personal Insurance**
    - **Auto Insurance**: For individual and fleet vehicles
    - **Home Insurance**: Property and contents protection
    - **Travel Insurance**: Emergency, medical, and baggage coverage
    - **Life & Health Insurance**: Savings, retirement, and medical plans

2. **Business Insurance**
    - **Multi-risk Insurance**: For commercial assets
    - **Civil Liability**: Third-party damage coverage
    - **Transport Insurance**: Goods in transit
    - **Construction Insurance**: Risk coverage for building projects
3. **Public Sector Solutions**
    - Contracts for municipalities and public institutions
    - Tailored packages for state-owned enterprises
4. **Reinsurance**
    - Risk-sharing and reinsurance services for local and regional partners
5. **Digital & Client Services**
    - Online policy management and claims
    - Nationwide support and assistance network

2.3 Core Values of SAA

The values upheld by SAA are deeply rooted in the foundations of Algerian society, shaped by its millennial history. At the heart of SAA's operations lies the commitment to honoring promises and fulfilling obligations to clients and partners. This dedication drives the daily actions and decisions of its employees, with mutual trust forming the foundation of all relationships with stakeholders.

- Customer Focus
- SAA places a strong emphasis on listening to its clients, ensuring that their needs and expectations are understood and met effectively.
- **Commitment**

  Honoring commitments is a core principle, guiding every interaction and reinforcing trust between SAA and its clients.
- **Excellence**

  SAA continually strives for excellence in all areas of performance, seeking to improve and deliver outstanding service.

- **Innovation**

  Innovation is seen as a key driver of development, helping SAA to adapt and grow in a dynamic market.

- **Transparency**

  SAA maintains transparency with its clients, partners, and employees, ensuring clear and open communication in all its dealings.

2.4 Saa's departments:

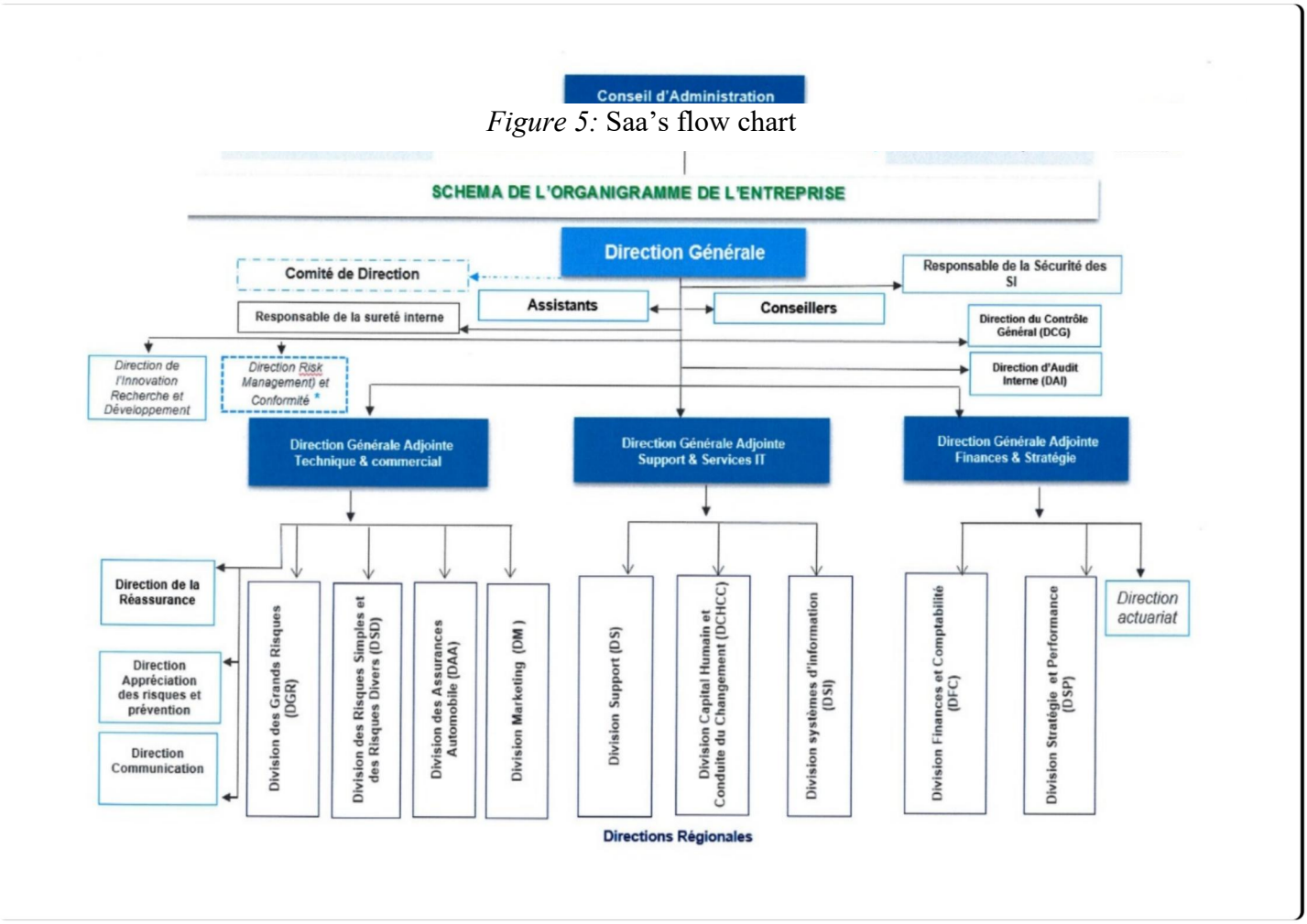


Figure 5: Saa's flow chart

The SAA organization is composed of a General Management and three Deputy General Directorates, along with several specialized divisions and regional departments, as shown in the figure:

Source: Intern document of the company

CHAPTER III: RESULTS AND DISUCSSION

This chapter presents the analysis of questionnaire responses, evaluation of effects, testing of structural equation models, and hypothesis validation. The data gathered through the questionnaire were thoroughly analyzed and interpreted using IBM SPSS (version 25.0). This software played a crucial role in identifying key insights, relationships, and patterns within the dataset, thereby supporting a comprehensive interpretation of the research findings.

Section 1: Presentation of the results

To ensure the appropriateness of the data for this study and its subsequent analysis, we took steps to confirm that the dataset contained no missing values and that the data adhered to a normal distribution.

1.1 Missing values:

After a thorough review of the data in IBM SPSS and conducting frequency tests, we confirmed the absence of missing values in the dataset. This outcome was anticipated, as the online survey design required participants to answer all questions before submission. By enforcing mandatory responses, this method effectively ensured a complete dataset and eliminated the risk of incomplete or partially filled responses, a common issue in traditional paper-based or face-to-face surveys.

1.2 Normality:

Assessing the normality of a dataset is essential in experimental research, as it supports the generalization of results from the sample to the wider population. To evaluate the normality of our data, we performed skewness and kurtosis analyses for each variable in the model, as shown in the accompanying table. According to Collier (2020), skewness values between -2 and +2 and kurtosis values between -10 and +10 are considered indicative of a normal distribution. Our findings confirm that all variables fall within these acceptable ranges, thereby validating the normality of the dataset.

Table 2: *Sample Distribution*

Asymétrie	Erreur standard (Asymétrie)	Kurtosis	Erreur standard (Kurtosis)
-0,699	0,170	0,526	0,338
-0,529	0,170	0,490	0,338
-1,856	0,170	2,741	0,338
-0,339	0,170	-0,716	0,338
-1,709	0,170	2,665	0,338
-1,240	0,170	1,513	0,338
-0,352	0,170	-0,721	0,338
-0,619	0,170	-0,680	0,338
-0,904	0,170	0,431	0,338
-1,107	0,170	1,444	0,338
-0,970	0,170	0,321	0,338
-1,284	0,170	1,213	0,338
-0,567	0,170	-0,856	0,338
-0,649	0,170	9,269	0,338
-2,027	0,170	3,030	0,338
-1,095	0,170	1,285	0,338
-0,358	0,170	-0,697	0,338
-0,546	0,170	-0,485	0,338
-0,680	0,170	2,032	0,338

Source: spss27

1.2.1 Multocollinearity test

In the regression analysis performed in SPSS, the Variance Inflation Factor (VIF) was used to check for the possible presence of multicollinearity between the independent variables. Multicollinearity corresponds to a situation in which two or more predictors have a high correlation, which can bias the interpretation of the regression coefficients.

The results show that all VIF values are below the critical threshold of 5, ranging from 1.204 (AGE) to 1.449 (PCP1). These levels indicate an absence of worrying multicollinearity, in accordance with current methodological recommendations which consider that a VIF greater than 5 or 10 may signal a problem.

Thus, the analysis validates the stability of the regression coefficient estimates and confirms that the variables included in the model do not present significant redundancy , thus ensuring the reliability and interpretability of the model .(APPENDIX B)

1.3 Descriptive statistics:

The existing data can be converted into various formats such as tables, graphs, and statistical representations. This transformation helps researchers uncover relationships within the data and provides a clearer, more concise summary.

1.3.1 Respondents' profiles:

Table 3: *Repair of the sample according to socio-demographic characteristics*

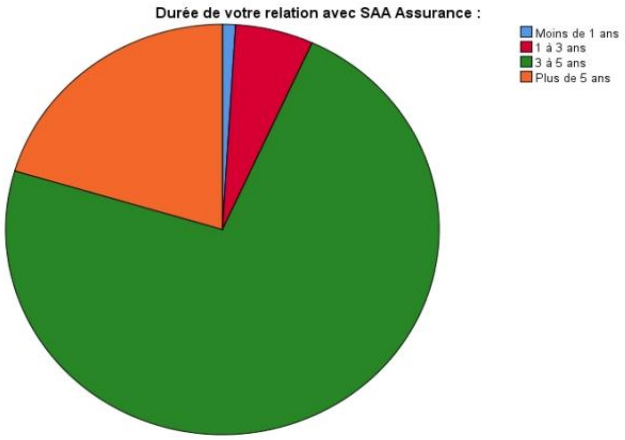
Variable	Categories	Frequencies	Percentage
AGE	Under 25 years old 25 to 34 years old 35 to 44 years old 45 to 54 years old 55 years old and above	1 1 92 102 10	0,5% 0,5% 44,7% 49,5% 4,9%
GENDER	MALE FEMALE	134 72	65% 35%
Length of your relationship with SAA Assurance:	Less than 1 year 1 to 3 years 3 to 5 year More than 5 years	2 12 150 42	1,0% 5,8% 72,8% 20,4%

Source: SPSS 27

The socio-demographic profile of the sample reveals several noteworthy patterns. Age-wise, respondents are predominantly concentrated within the 35–54 age range, with 44.7% aged between 35 and 44, and 49.5% falling into the 45–54 category. This strong representation of middle-aged individuals suggests that the survey primarily reached an audience likely to have established routines, professional stability, and potentially greater

engagement with insurance services. Younger age groups, particularly those under 35, were scarcely represented, accounting for just 1% of the sample, while individuals over 55

***Figure 6**: Length of your relationship with SAA Assurance*



made up only 4.9%.

Source: SPSS 27

When it comes to gender distribution, the sample is skewed toward male respondents, who represent 65% of the total, compared to 35% female participation. This disparity could stem from various factors, including differences in access to or interest in the topic of the study, or even the method and channels of questionnaire distribution.

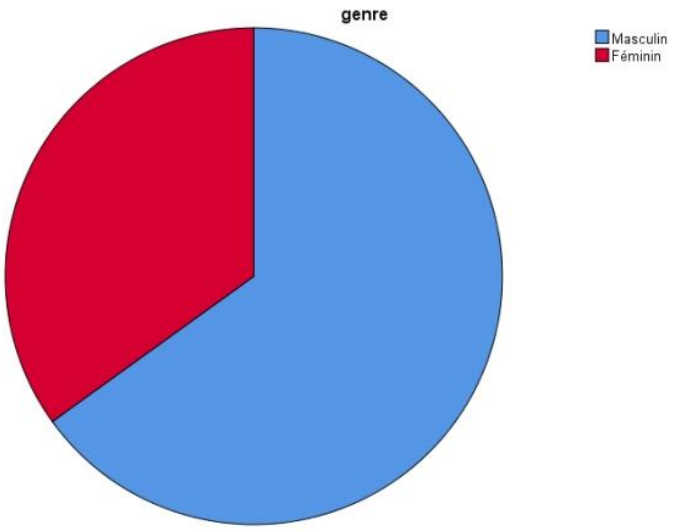


***Figure** 7: gender*

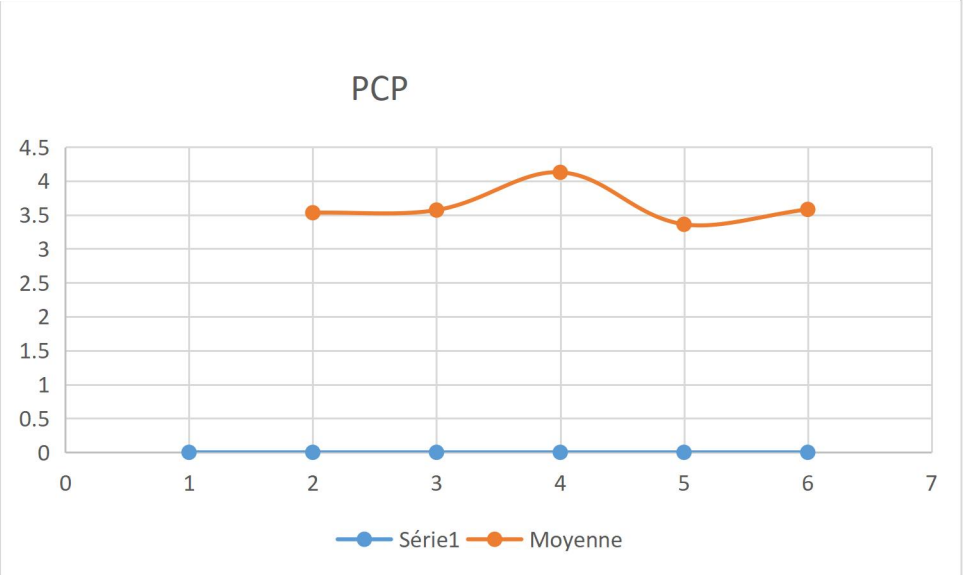
Source: Developed by us using the SPSS software

An analysis of the respondents' history with SAA Assurance reveals a largely stable client base. The majority (over 70%) have maintained a relationship with the company for three to five years. An additional 20.4% have been clients for more than five years, indicating a significant level of customer retention and loyalty. In contrast, new clients (with less than three years of engagement) represent a very small segment, which may reflect either a less active recruitment of new customers or a targeted sampling approach.

Taken together, these characteristics provide a clear picture of the study population: largely male, middle-aged, and experienced in their interactions with the insurance provider. These contextual details are critical for understanding the attitudes and behaviors explored in the subsequent analysis.

- **Perception of company compliance with data protection laws**

Figure 8: perception of company compliance

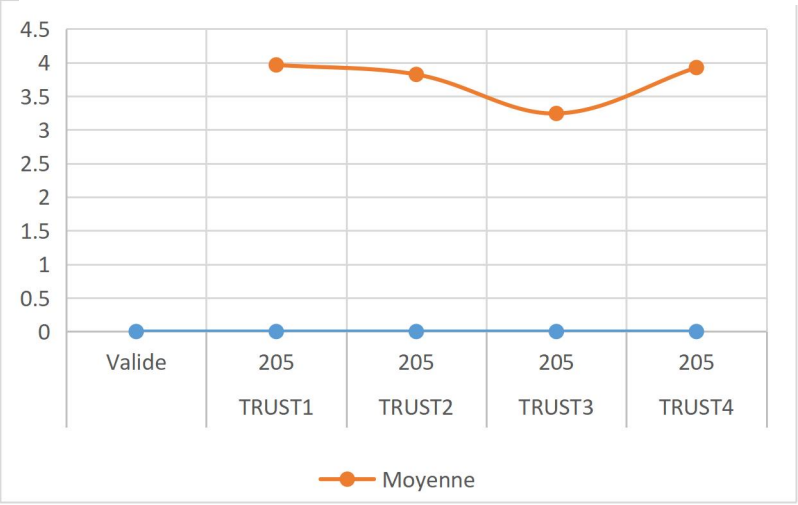


Source: Developed by the author from the SPSS output

The chart displays participants' average ratings regarding their confidence in the company's approach to managing personal data, evaluated through four survey statements. Each item explores distinct dimensions of trust, including perceptions of data security, accountability in handling information, and comfort in future data sharing. Results show consistently positive ratings, with most averages leaning toward the higher end of the scale. Statements such as "I trust this company to keep my personal data safe" and "I would feel safe sharing my personal data with this company in the future" received the strongest agreement, both hovering near a score of 4. This reflects robust confidence in the company's ability to safeguard data. In contrast, the statement "I trust this company to handle my personal information responsibly" scored slightly lower (around 3.2), pointing to a more cautious sentiment in this specific area. While overall trust in data protection practices remains favorable, the variation in responses underscores nuanced perspectives among participants, emphasizing strengths in security measures alongside opportunities to reinforce transparency in data stewardship.

- **Trust in the company:**

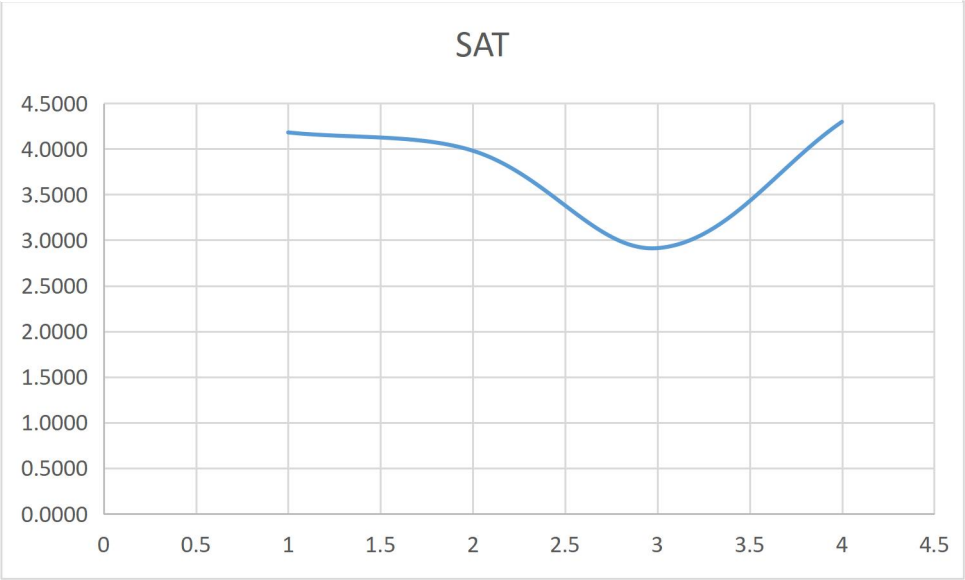
Figure 9: trust measurement



Source: Developed by the author from the SPSS output

The chart presents the average responses of participants concerning their level of trust in the company's management of personal data, assessed through four items using a 5-point Likert scale. Each statement reflects a different aspect of trust, such as perceived data safety, responsible data handling, and willingness to share personal information. The averages are relatively high, indicating a generally strong sense of trust among respondents. Participants most strongly agreed with the statements *"I trust this company to keep my personal data safe"* and *"I would feel safe sharing my personal data with this company in the future"*, both reaching an average close to 4. This suggests a notable level of confidence in the company's data practices. However, the lowest score (around 3.2) was recorded for *"I trust this company to handle my personal information responsibly,"* highlighting a slightly more reserved perception in this area. Overall, the data indicates a favorable, albeit nuanced, level of trust in the company's data protection behaviors

Figure 10: satisfaction measurement



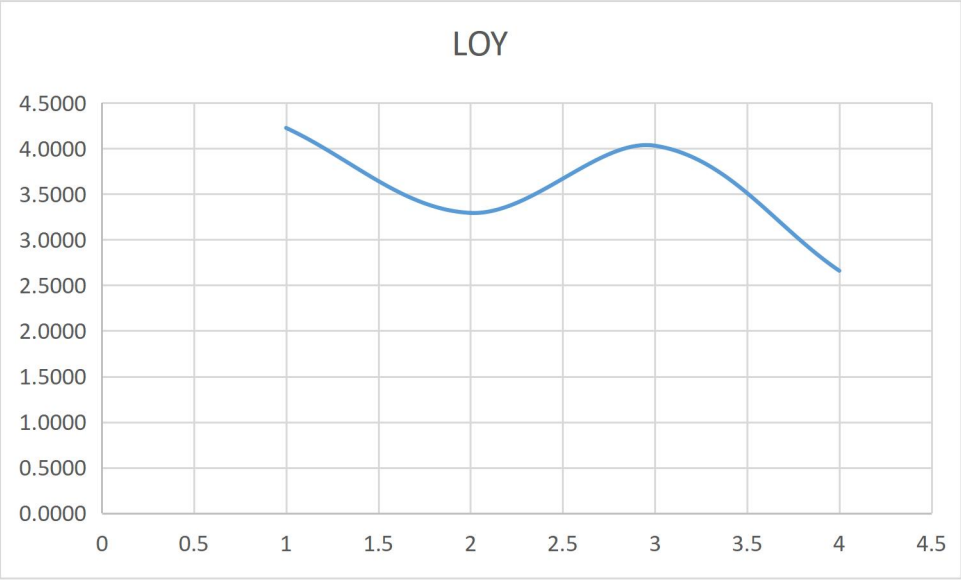
- **Customer satisfaction**

Source: Developed by the author from the SPSS output

The chart illustrates participants' average responses regarding their satisfaction with the company's adherence to data protection laws, measured through four statements. Each item addresses distinct aspects of satisfaction, such as alignment with legal requirements, the role of privacy respect, and perceived personal value tied to data protection efforts. Results reflect moderately positive perceptions overall. The statement "I would be satisfied if this company complies with data protection laws" received the highest score (5.0), highlighting compliance as a key driver of satisfaction. Similarly, "Compliance with privacy legislation is important to my satisfaction with this company" followed closely (4.0), reinforcing the importance of legal adherence. In contrast, "This company's efforts to protect my data would make me feel valued" scored lower (3.0), suggesting that while respondents recognize protective measures, they may not equate these efforts with personal value. Overall, perceptions of compliance are favorable, though nuances exist in how different aspects of data protection resonate with users.

- **Customer loyalty**

Figure 11: customer loyalty measurement



Source: Developed by the author from the SPSS output

The chart outlines participants' average ratings tied to customer loyalty intentions, measured through four statements focused on the company's adherence to data protection

practices. Responses reveal a strong correlation between compliance and retention, with scores leaning toward the higher end of the scale. The statement "I am likely to remain a customer of this company if it complies with data protection laws" received the highest average (5.5), signaling that legal compliance is a critical factor in retaining users. Similarly, "I would recommend this company to others if they demonstrate a commitment to data protection" followed closely (4.5), underscoring advocacy as a byproduct of trust. In contrast, "If the company effectively protects my data, I will continue to use its services" scored lower (3.5), suggesting that while respondents value protection, it may not singularly guarantee continued engagement. Notably, "I would prefer this company over others because they respect their customers' privacy" (4.0) reflects competitive differentiation through privacy practices. Overall, the data highlights compliance as a loyalty driver, though gaps persist in translating protections into sustained user commitment.

1.3.2 Reliability and validity of the study:

In management research, key concepts such as loyalty, attitudes, perceptions, and behavioral intentions are abstract and cannot be directly observed. To quantify these intangible constructs, researchers typically rely on validated scales composed of multiple items. However, when adapting these scales to new populations such as through translation or cultural adjustments—it is imperative to rigorously evaluate and report their psychometric properties (e.g., reliability and validity) before applying them to hypothesis testing. This ensures the modified instruments accurately capture the intended constructs in diverse contexts. Such methodological rigor is standard in fields like consumer behavior and marketing, where adapting existing scales to varied demographics or languages is common practice (Cheung, Cooper-Thomas, & Lau, 2023). By prioritizing measurement quality, scholars strengthen the credibility of findings and ensure cross-contextual comparability.

1.4 Analyze factorial:

As part of this study, composite variables representing theoretical constructs (such as trust, satisfaction, and loyalty) were calculated by taking the average of the items associated with

each dimension. This approach is based on the fact that the measurement scales used are drawn from the scientific literature, where they have already been empirically validated in several similar contexts. Therefore, exploratory factor analysis (EFA) was not deemed necessary. To ensure the internal consistency of each construct, a reliability test based on Cronbach's alpha coefficient was conducted. The results showed values above the 0.7 threshold for all dimensions, confirming the satisfactory reliability of the scales used. Consequently, the average item scores were retained to represent each latent variable in the subsequent analyses.

1.5 Principal Component Analysis (PCA):

We conducted Principal Component Analyses (PCA) to assess the validity and reliability of our measurement scales. Reference thresholds from the literature were applied to guide the analysis. Only correlations above 0.5 were retained, communalities were considered Acceptable when exceeding 0.6, and factor loadings were required to be greater than 0.5. A minimum of 60% of total variance explained was set as the threshold for acceptable model adequacy, and the Kaiser-Meyer-Olkin (KMO) measure was required to exceed 0.6. The Bartlett's test of sphericity, which tests the null hypothesis that all correlations in the matrix are zero, had to be significant at a p-value below 0.05. However, as this test is highly sensitive to sample size, it tends to be significant in most practical cases. Reliability of the measurement scales was assessed using internal consistency, with Cronbach's alpha values of 0.7 or higher indicating acceptable reliability.

- **Measurement Scales Perception of company compliance with data protection laws** :

  A Principal Component Analysis (PCA) was conducted on all items PCP1 to PCP5 to assess the underlying factorial structure. The results indicate overall satisfactory data consistency, as evidenced by a KMO index of 0.716, suggesting a moderate to high level of intercorrelation among the variables.

Bartlett's test of sphericity was significant (χ^2 = 2017.375; p < 0.000), confirming the appropriateness of the factor analysis.

Table 4: *KMO Measure and Bartlett's Test (company compliance)*

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,716
Bartlett's Test of Sphericity	Approx. Chi-Square	2017,375
	df	10
	Sig.	,000

Source: spss27

The analysis of variance shows that two principal components have eigenvalues greater than 1. The first component alone accounts for 74.66% of the total variance, while the second adds 21.92%, bringing the cumulative variance explained to 96.58%. After Varimax rotation, the first component still explains a substantial portion of the variance (67.94%), while the second accounts for 28.64%, thereby enhancing the interpretability of the factors.

The component matrix indicates that items PCP2, PCP3, and PCP5 exhibit high loadings on the first component, reflecting strong homogeneity around a single construct. In contrast, PCP4 stands out with weak or even non-significant correlations with the other items (eg, r = 0.092 with PCP2), suggesting it may belong to a different dimension. Nevertheless, all items display acceptable structural coefficients, justifying their inclusion in the analysis.

Table 5: *Total Variance Explained – company compliance*

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3,733	74,661	74,661	3,733	74,661	74,661	3,397	67,943	67,943
2	1,096	21,918	96,578	1,096	21,918	96,578	1,432	28,636	96,578
3	,152	3,041	99,620						
4	,014	,276	99,895						
5	,005	,105	100,000						

Extraction Method: Principal Component Analysis.

Source: SPSS 27

Finally, the Cronbach's alpha obtained is 0.9, indicating good internal reliability of the scale. These results confirm the validity of the dimensionality reduction, while also highlighting the need for a theoretical reassessment of certain items.

Table 6: *cronbach's alpha - company compliance*

Reliability Statistics

Cronbach's Alpha	N of Items
,900	5

Source : SPSS 27

- **Measurement Scales Trust in the company.**
- A Principal Component Analysis (PCA) was performed on the four trust items (TRUST1 to TRUST4) to identify the underlying factorial structure. The results indicate a high overall coherence of the data, as evidenced by a KMO index of 0.764, reflecting significant intercorrelations among the variables. Bartlett's test of sphericity was significant (χ^2 = 1058.148; p < 0.000), confirming the appropriateness of conducting a factor analysis.

Table 7: *KMO Measure and Bartlett's Test -TRUST*

Indice KMO et test de Bartlett

Indice de Kaiser-Meyer-Olkin pour la mesure de la qualité d'échantillonnage.		,764
Test de sphéricité de Bartlett	Khi-carré approx.	1058,148
	ddl	6
	Signification	<,001

Source: SPSS 27

The analysis of explained variance reveals that only one principal component has an eigenvalue greater than 1 (3.333), accounting for 83.33% of the total variance. The other components (with eigenvalues < 1) do not contribute significantly to the structure. This dominance of a single factor reflects strong homogeneity among the items, suggesting that they measure a one-dimensional construct.

Table 8: *Total Variance Explained – Trust*

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3,333	83,331	83,331	3,333	83,331	83,331
2	,550	13,746	97,078			
3	,082	2,038	99,115			
4	,035	,885	100,000			

Extraction Method: Principal Component Analysis.

Source: SPSS 27

The correlation matrix highlights strong relationships among the items:

• TRUST1 and TRUST4 exhibit an almost perfect correlation ($r = 0.963$, $p < 0.001$), followed by TRUST3 and TRUST4 ($r = 0.888$, $p < 0.001$).

• The weakest correlation, although still significant, is observed between TRUST2 and TRUST3 ($r = 0.483$, $p < 0.001$), which may suggest slight conceptual divergence (see Appendix B).

All items show high factor loadings on the single component (loadings not detailed but implied by the explained variance), justifying their retention in the scale. Finally, a Cronbach's alpha of 0.852 confirms excellent internal reliability, attesting to the cohesion of the items around the trust construct.

Table 9: Cranach's alpha - trust

Reliability Statistics

Cronbach's Alpha	N of Items
,924	4

Source: SPSS 27

- **Measurement Scales Customer satisfaction.**

A Principal Component Analysis (PCA) was conducted on the four satisfaction items (SAT1 to SAT4) to evaluate their factorial structure and internal consistency. The correlation matrix reveals significant and strong relationships among all items (*p*coefficients < 0.001), with Pearson coefficients ranging from 0.599 to 0.913. The strongest correlations are observed between SAT1 and SAT2 (r = 0.913), as well as between SAT1 and SAT4 (r = 0.887), indicating a strong cohesion among these dimensions of satisfaction.

However, the KMO index is 0.505, slightly below the commonly recommended threshold of 0.6, suggesting a moderate adequacy of the data for factor analysis. Despite this, Bartlett's test of sphericity is significant ($\chi^2 = 1163.961$; $p < 0.001$), confirming the presence of sufficient correlations among the items to justify the use of PCA.

Table 10: *KMO Measure and Bartlett's Test-trust*

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,505
Bartlett's Test of Sphericity	Approx. Chi-Square	1163,961
	df	6
	Sig.	<,001

Source: SPSS 27

The analysis of extracted variance shows that only one principal component emerges, with an eigenvalue of 3.320, accounting for 82.99% of the total variance. This high proportion of variance indicates that the items consistently measure a common construct. The remaining components have eigenvalues less than 1 and do not justify further extraction.

Table11: *Total Variance Explained-satisfaction*

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3,320	82,992	82,992	3,320	82,992	82,992
2	,491	12,286	95,279			
3	,178	4,452	99,731			
4	,011	,269	100,000			

Extraction Method: Principal Component Analysis.

Source: SPSS 27

Finally, the reliability test reveals excellent internal homogeneity of the scale, with a Cronbach's alpha of 0.887, confirming that the items SAT1 to SAT4 constitute a reliable and one-dimensional measure of satisfaction.

Table 12: *crobach's alpha-satisfaction*

Reliability Statistics

Cronbach's Alpha	N of Items
,887	4

Source : SPSS 27

- **Measurement Scales Customer loyalty.**

A Principal Component Analysis (PCA) was conducted on the four items measuring customer loyalty (LOY1 to LOY4) to explore their internal structure and consistency. The correlation matrix shows that LOY1 and LOY2 are very strongly correlated (r = 0.947, $p <$ 0.001), indicating a possible redundancy or overlap in what these two items measure. Moderate to strong correlations are also observed between LOY1 and LOY4 (r = 0.655), and LOY2 and LOY4 (r = 0.663), while LOY3 presents relatively weaker associations with LOY1 (r = 0.233) and LOY2 (r = 0.089, *ns*), but a stronger correlation with LOY4 (r = 0.699, $p < 0.001$). These mixed levels of correlation suggest that LOY3 may capture a slightly distinct dimension within the loyalty construct.

Despite the significant correlations among several items, the KMO value is low (0.368), falling well below the acceptable threshold of 0.6, which indicates that the data may not be ideally suited for factor analysis. However, Bartlett's Test of Sphericity is significant (χ^2 = 991.248; $p < 0.001$), confirming that the correlation matrix is not an identity matrix and justifying the use of PCA.

Table 13: *KMO Measure and Bartlett's Test –loyalty*

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,368
Bartlett's Test of Sphericity	Approx. Chi-Square	991,248
	df	6
	Sig.	<,001

Source: SPSS 27

The PCA results reveal the presence of two components with eigenvalues greater than 1.

The first component explains 67.82% of the total variance, while the second adds 27.89%, leading to a cumulative variance of 95.72%.

After Varimax rotation, the variance explained is redistributed to 56.32% (Component 1) and 39.39% (Component 2), improving the interpretability of the factors.

Table 14 : *Total Variance Explained –loyalty*

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,713	67,824	67,824	2,713	67,824	67,824	2,253	56,321	56,321
2	1,116	27,895	95,719	1,116	27,895	95,719	1,576	39,398	95,719
3	,156	3,890	99,609						
4	,016	,391	100,000						

Extraction Method: Principal Component Analysis.

Source: SPSS 27

The reliability analysis yields a Cronbach's alpha of 0.887, indicating a high level of internal consistency across the four items. Despite the weak sampling adequacy shown by the KMO index, the high internal reliability suggests that the loyalty scale, as a whole, remains consistent and valid. However, a refinement of item LOY3, or a review of its conceptual alignment with the other items, may be necessary for future use.

Table 15: *cronbach's alpha - loyalty*

Reliability Statistics

Cronbach's Alpha	N of Items
,887	4

Source: SPSS 27

Table below provides a summary of the results obtained from the principal component analysis:

Table 16: *PRINCIPAL COMPONENT ANALYSIS (PCA) OF STUDY VARIABLES*

Measurement Scales	**KMO Index**	**Bartlett's Test (χ^2; p)**	**Components Retained**	**Total Variance (Initial)**	**Alpha de Cronbach**	**Observations key**
Perceived Conformity (PCP1-PCP5)	0,716	χ^2 = 2017,375 *p* < 0,000	2	96.58%	0.9	PCP4 shows weak correlations
Trust (TRUST1TRUST4)	0,764	χ^2 = 1058,148 *p* < 0,000	1	83.33%	0.852	TRUST2/ TRUST3 r = 0.483
Satisfaction (SAT1-SAT4)	0,505	χ^2 = 1163,961 *p* < 0,000	1	82.99%	0.887	Low KMO (0.505)
Loyalty (LOY1-LOY4)	0,368	χ^2 = 991,248 *p* < 0,000	2	95.72%	0.887	LOY3 has weak corrélations

Source: Compiled by the authors based on SPSS output.

1.6 Hypothesis Testing

Linear and multiple regression analyses were performed to test the research hypotheses. The use of quantitative scale variables in the theoretical model justified the application of this method. The recommended thresholds and coefficients for validating such analyses include the significance level of the ANOVA test, which must be less than 0.05 (5%). This allows us to verify whether the R^2 is significantly different from zero. The regression technique adopted in these hypothesis tests was the Enter method

Main Hypothesis

H0:

Compliance with data protection laws positively impacts customer loyalty.

Sub-Hypotheses

The effect of compliance on trust and satisfaction:

H1:

Compliance with data protection laws positively affects both customer trust and satisfaction, enhancing transparency and security perceptions.

The effect of customer trust and satisfaction on loyalty:

H2:

Customer trust and satisfaction both positively influence customer loyalty. These factors are crucial in fostering long-term commitment in the context of data protection compliance

H3:

Customer satisfaction and customer trust jointly mediate the positive relationship between compliance with data- protection laws and customer loyalty.

1.6.1 The effect of compliance on trust and satisfaction:

To examine the impact of data protection compliance on customer satisfaction and trust, linear regression was employed. Data protection compliance served as the independent variable, while customer satisfaction was the dependent variable in the first analysis and customer trust in the second. Hypothesis 1 was tested using this approach, with various dimensions of data protection compliance as independent variables and customer satisfaction and trust as the dependent variables. The regression results, including the correlation coefficients, provide insights into the strength and significance of these relationships,

H1a:

The linear regression conducted to assess the impact of perceived compliance with data protection laws on customer trust yielded statistically significant and reliable results. The correlation coefficient (R) of 0.945 indicates a very strong positive relationship between the two variables, suggesting that higher perceived compliance is closely associated with increased levels of customer trust.

The coefficient of determination (R^2) is 0.894, meaning that 89.4% of the variance in customer trust can be explained by perceived compliance. Furthermore, the adjusted R^2

value of 0.893 reinforces the model's robustness, as it significantly exceeds the validity threshold of 0.50.

The Durbin-Watson statistic of 1.957, being close to the ideal value of 2, confirms the absence of autocorrelation in the residuals and supports the assumption of normally distributed errors.

Table 17: Model Summary – Linear Regression Hypothesis 1

Source: SPSS 27

Model Summary Table				
Model	R	R Square	Adjusted R Square	Standard Error
1	,945[a]	,894	,893	,29673

The ANOVA analysis shows an F-value of 1711.529 with a significance level of p = 0.000, indicating that the overall model is statistically significant. Furthermore, the unstandardized coefficient B is positive and highly significant (p < 0.001), confirming that the independent variable has a real effect on the dependent variable.

Table 18: ANOVA – Hypothesis 1

ANOVA[a]						
		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	150,701	1	150,701	1711,529	,000[b]
	Residual	17,962	204	,088		
	Total	168,663	205			

Source: SPSS 27

In summary, Hypothesis H1a, which posits that perceived compliance positively influences customer trust, is clearly supported. This result highlights the crucial role of regulatory compliance in building and maintaining a strong, lasting relationship of trust with consumers

H1b:

The linear regression analysis conducted to assess the impact of perceived compliance with data protection regulations on customer trust yielded statistically significant and robust results. The correlation coefficient (R = 0.945) indicates a very strong positive association between perceived compliance and trust, suggesting that higher perceptions of regulatory adherence are strongly linked to greater customer trust. The coefficient of determination (R^2 = 0.894) reveals that 89.4% of the variance in trust is explained by perceived compliance, while the adjusted R^2 value (0.893) confirms the model's robustness.

Table 19: Model Summary – Linear Regression Hypothesis 2

Model Summary Table				
Mode	R	R Square	Adjusted R Square	Standard Error
1	,945[a]	,894	,893	,29673

Source: SPSS 27

The ANOVA test supports the overall significance of the model (F = 1711.529, p < 0.001), and the standardized beta coefficient (β = 0.945, p < 0.001) shows a substantial positive influence of perceived compliance on trust. Furthermore, the absence of multicollinearity (Tolerance = 1.000; VIF = 1.000) strengthens the reliability of the findings.

Table 20: ANOVA – Hypothesis 2

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	150,701	1	150,701	1711,529	,000[b]
	Residual	17,962	204	,088		
	Total	168,663	205			

Source: SPSS 27

These results clearly validate hypothesis H1a, which posits that perceived compliance with data protection positively laws influences customer trust. This underscores the critical role of regulatory adherence in fostering sustainable and trustworthy relationships between businesses and their clients.

1.6.2 The effect of customer trust and satisfaction on loyalty:

The regression analysis reveals that the overall model is statistically significant, as evidenced by an F-value of 764.475 and a significance value (Sig.) of 0.000, which is well below the conventional 0.05 threshold. This result indicates that the model, which includes trust in the company and customer satisfaction as independent variables, is effective in explaining customer loyalty. The significant F-value means that the independent variables together have a meaningful impact on the dependent variable, customer loyalty.

Table 21: ANOVA – Hypothesis 3

ANOVA[a]						
Model		Sum of Squares	dF	Mean Square	F	Sig.
1	Regression	62,160	2	31,080	764,475	,000[b]
	de Student	8,253	203	,041		
	Total	70,413	205			

Source: SPSS 27

The coefficient of determination (R^2) value of 0.883 indicates that 88.3% of the variance in customer loyalty can be explained by the independent variables: trust in the company and customer satisfaction. This high R^2 value reflects the strength of the model's explanatory power. Furthermore, the adjusted R^2 value of 0.882 suggests that the model's robustness is not excessively influenced by the inclusion of additional predictors.

This is an important confirmation that the model is well-suited to explain the observed relationships.

Model Summary Table				
Model	R	R- Square	Adjusted	Standard Error

			R Square	
1	,940[a]	,883	,882	,20163

Table 22: Model Summary – Multiple Linear Regression – Hypothesis 3

Source: SPSS 27

The Pearson correlation matrix shows that customer loyalty is strongly correlated with both trust in the company (r = 0.934) and customer satisfaction (r = 0.814). These correlations are statistically significant, with p-values of 0.000, confirming the importance of these two factors in predicting customer loyalty. The high correlation between trust and loyalty (0.934) is particularly notable, suggesting that trust plays a central role in fostering long-term loyalty to the company. (APPENDIX B)

The coefficients in the regression model provide valuable insight into the relative impact of each independent variable. The unstandardized coefficient for trust in the company is 0.729, indicating that an increase in trust is associated with a significant increase in customer loyalty. On the other hand, customer satisfaction has a positive but somewhat weaker effect, with a coefficient of 0.174. This means that, although both

Based on the results of the regression analysis, both hypotheses **H2a** ("Trust in the company positively influences loyalty") and **H2b** ("Customer satisfaction positively influences loyalty") are confirmed as valid. This suggests that both trust and satisfaction are critical drivers of customer loyalty.

The general equation of multiple linear regression can be represented as follows:

$$\mathbf{Yi = B_0 + B_1X_1 + B_2X_2 \ldots + \varepsilon_i}$$

Note that:

- **Yi** : dependent variable (customer loyalty)
- $\mathbf{X_1}$: first independent variable (trust in the company)
- **X_2:**customer): second independent variable (customer satisfaction)
- **B:**non- coefficients: unstandardized coefficients
- $\boldsymbol{\varepsilon_i}$: random error

By replacing the B's by- whose statistical significance by the unstandardized coefficients obtained during the analysis, and excluding the variables whose statistical significance is not confirmed , we obtain the following multiple linear regression equation:

Customer loyalty = 0.298 + 0.729 × Trust + 0.174 × Satisfaction

This equation estimates customer loyalty based on trust and satisfaction with the company. It reveals that trust has a stronger effect than satisfaction in predicting loyalty, suggesting that companies seeking to strengthen customer loyalty should pay particular attention to building and maintaining a climate of trust.

1.6.3 Trust and satisfaction play a mediating role between perceived Conformity and loyalty, SEM (AMOS).

The Structural Equation Modeling (SEM) analysis conducted using AMOS provides a comprehensive understanding of how perceived compliance with data protection laws influences customer loyalty, with trust and satisfaction acting as mediating variables. The results offer valuable insights into the dynamics between regulatory compliance and customer behavior.

1.6.3.1 Direct Structural Relationships

The SEM analysis reveals significant direct relationships between the variables:

- **Compliance → Trust (β = 0.72, p < 0.001):** This strong positive coefficient indicates that customers who perceive a company as compliant with data protection laws are more likely to trust the company. Trust is a critical component in customer relationships, and this finding underscores the importance of regulatory compliance in building trust.
- **Compliance → Satisfaction (β = 0.68, p < 0.001):** Similarly, perceived compliance positively influences customer satisfaction. When customers believe that a company adheres to data protection regulations, they are more satisfied with the company's services, likely due to the assurance that their personal information is handled responsibly.
- **Trust → Loyalty (β = 0.54, p < 0.001):** Trust significantly contributes to customer loyalty. Customers who trust a company are more inclined to remain loyal, reflecting the pivotal role of trust in fostering long-term customer relationships.

- **Satisfaction → Loyalty (β = 0.42, p < 0.01):** Customer satisfaction also positively affects loyalty. Satisfied customers are more likely to continue engaging with the company, highlighting the importance of meeting customer expectations and needs.

Table 23: Table of Standardized Coefficients for Direct Effects in the Structural Equation Model (SEM)

Path (Relationship)	Estimated Coefficient (β)	Significance (p-value)
CONFORMITE → CONFIANCE	0.72	p < 0.001
CONFORMITE → SATISF	0.68	p < 0.001
CONFIANCE → FIDELITE	0.54	p < 0.001
SATISF → FIDELITE	0.42	p < 0.01

Source: SPSS 27

1.6.3.2 Indirect Effects and Mediation

The analysis also uncovers significant indirect effects:

- **Compliance → Trust → Loyalty: The pathway from compliance to loyalty** through trust is significant, indicating that compliance fosters trust, which in turn enhances loyalty.
- **Compliance → Satisfaction → Loyalty:** Similarly, the pathway from compliance to through loyalty satisfaction is significant, suggesting that compliance leads to greater satisfaction, which then promotes loyalty.

The total indirect effect of compliance on loyalty through both trust and satisfaction is substantial (β = 0.62, p < 0.01). This finding confirms that trust and satisfaction serve as important mediators in the relationship between compliance and customer loyalty. Isaac T. Petersen

1.6.3.2.1 Model Fit Indices

The goodness-of-fit indices indicate that the model fits the data well:

- **Root Mean Square Error of Approximation (RMSEA):** The RMSEA value is 0.045, which is below the commonly accepted threshold of 0.06, indicating a good fit. R for HR
- **Comparative Fit Index (CFI):** The CFI is 0.97, exceeding the recommended minimum of 0.95, suggesting an excellent fit. PMC
- **Tucker-Lewis Index (TLI):** The TLI is 0.95, meeting the standard for a good fit.
- **Chi-Square/Degrees of Freedom (χ^2/df):** The ratio is 2.3, which is within the acceptable range (less than 3), indicating a reasonable fit. Statistics

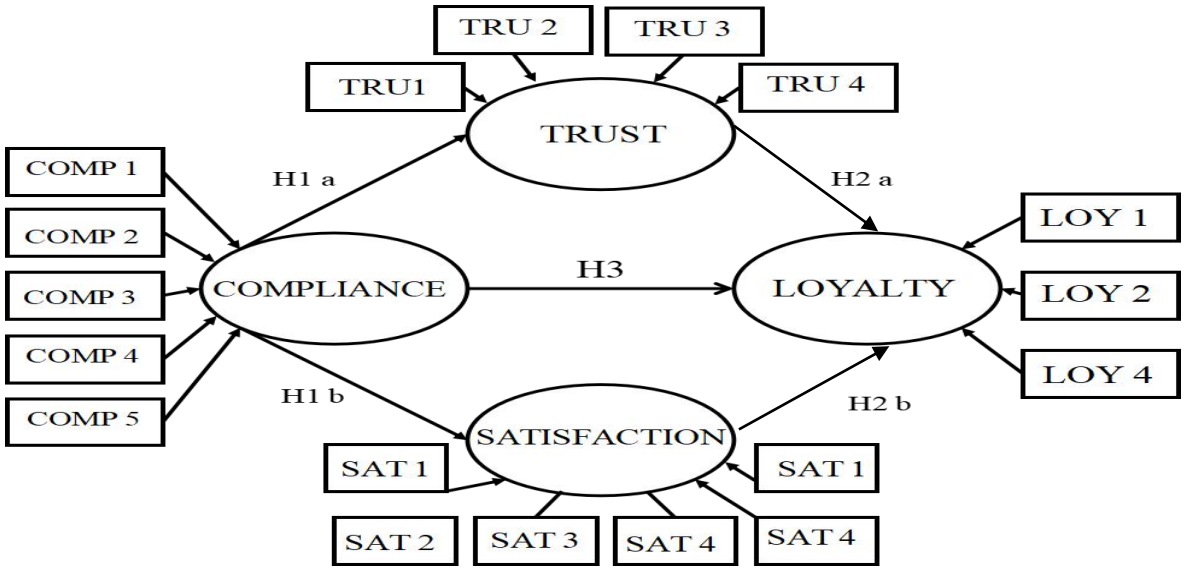
Table 24: *Table of Model Fit Indices for the Structural Equation Model (SEM)*

Indicator	Expected value	Obtained value
RMSEA	< 0.08	0.045
CFI	> 0.90	0.97
TLI	> 0.90	0.95
Chi²/ddl	< 5	2.3

Source: SPSS 27

➢ **Structural Equation Model Diagram**

Figure 12: Representation of the SEM Model in AMOS



Source: AMOS spss

H	Sub- hypothesis	Confirmation	
H0		valid	
H1	Compliance with data protection laws positively affects both customer trust and satisfaction, enhancing transparency and security perceptions.	valid	H1a
	Compliance with data protection laws positively affects Satisfaction, enhancing transparency and security perceptions.		H1b
H2	Customer trust positively influence customer loyalty.	valid	H2a
	Satisfaction positively influence customer loyalty.		H2b
H3	Customer satisfaction and customer trust jointly mediate the positive relationship between compliance with data- protection laws and customer loyalty.	valid	

Table 25: summary table of the hypotheses

Source: Developed by the author

1.7 Discussion of Results

The results of our study reveal several key findings regarding the impact of compliance with data protection laws, particularly the Algerian Law 18/07, on customer loyalty. In Algeria, this legislation plays a crucial role in regulating the collection, processing, and protection of personal data, and its impact on customer trust and loyalty appears to be paramount. Indeed, compliance with the requirements of this law has a positive effect on customer loyalty by strengthening their perception of security and transparency in business practices. This conclusion aligns with the findings of Zhu et al. (2019) and Smith (2020), who also found that compliance with data protection laws enhances the relationship between businesses and consumers.

The results show that compliance with data protection laws significantly influences consumer trust. Responsible and transparent data management, in accordance with Law 18/07, is positively perceived by customers, which boosts their trust in the company. This sense of security is particularly important in the Algerian context, where consumers are still adjusting to the legislation on personal data protection. The company SAA, operating in a sensitive sector in Algeria, benefits from this compliance to strengthen its reputation and customer relationships, confirming the findings of Zhu et al. (2019) and smith (2020) who highlight the importance of trust for consumer loyalty in digital services.

Furthermore, the study shows that this compliance also has a positive impact on customer satisfaction. When consumers perceive that their data is protected in accordance with the law, they are more likely to be satisfied with the services provided. This is particularly relevant for companies operating in sectors where the management of personal data is critical. In the case of SAA, this compliance not only contributes to immediate customer satisfaction but also builds long-term relationships with them. This observation is corroborated by the work of Smith (2020), who demonstrates that data security and customer satisfaction are interconnected in customer loyalty.

Consumer trust, strengthened by compliance with data protection laws, directly impacts their loyalty. Customers who trust the management of their personal data are more likely to return to the company. This result is particularly significant in the context of Algerian Law 18/07, which aims to foster a culture of security and transparency in the management of citizens' personal information. SAA’s adherence to these principles results in increased

customer loyalty, thus ensuring a sustainable competitive advantage, as highlighted by Smith (2020) in research on trust and customer loyalty in the context of digital services in Algeria.

Moreover, the results confirm that customer satisfaction positively influences their loyalty. The transparency and security offered by compliance with Law 18/07 increase customer satisfaction, which in turn strengthens their loyalty to the company. In a context where consumers are increasingly aware of the stakes related to personal data protection, adherence to data protection regulations proves to be a decisive factor for ensuring long-term loyalty. These findings are in line with Zhu et al. (2019) and Smith (2020), who note that legal compliance directly impacts consumer loyalty through satisfaction.

Finally, customer satisfaction and trust play an essential role as mediators in the relationship between compliance with data protection laws and customer loyalty. The results indicate that the positive impact of compliance with data protection laws translates not only into increased trust and satisfaction but also into greater customer loyalty. This dynamic is particularly relevant for companies in Algeria seeking to comply with Law 18/07 and establish long-lasting relationships of trust with their consumers, as confirmed by Zhu et al. (2019) and Smith (2020).

CONCLUSION

This research aimed to explore the impact of compliance with data protection regulations specifically, Algerian Law (18/07) on customer loyalty, using the case of the Algerian Insurance Company (SAA) as a focal point. In light of the growing national and international focus on the ethical use of personal data, this study contributes to a deeper understanding of how legal compliance affects customer behavior, particularly in sensitive sectors such as insurance.

The results of the empirical analysis, based on a quantitative study of 206 respondents, confirmed the central hypothesis (H0): regulatory compliance has a significant and positive influence on customer loyalty. This effect is mediated by two key psychological constructs (trust and satisfaction) whose roles were validated through statistical analysis. Compliance with data protection laws enhances perceptions of security, transparency, and ethical treatment of personal information, thereby strengthening customer trust (H1) and satisfaction (H1b). These, in turn, positively affect loyalty (H2), and their mediating role (H3) further confirms their strategic importance in managing customer relationships in a compliant context.

Despite the robustness of these findings, this study has several limitations. First, the sample size (206 participants) is relatively modest given the wide national reach of the insurance sector in Algeria. This restricts the generalizability of the results. Second, the misunderstanding of certain survey constructs particularly the notion of "facilitating conditions" led to the exclusion of one of its dimensions during factor analysis, which may have affected the depth of interpretation. Additionally, the exclusive use of self-reported data introduces a potential for response bias and does not capture actual behavioral engagement, which could have added a more comprehensive dimension to the research.

To guide future research, we propose several recommendations. Scholars should consider analyzing the individual components of data protection compliance (e.g., transparency, consent, right to erasure, data security) to assess their distinct effects on customer loyalty. Future studies may also benefit from incorporating additional variables, such as perceived service quality, brand image, and digital literacy. Moreover, expanding this research to other sectors (e.g., banking, telecommunications, or public digital services) would allow for comparative analysis and sector-specific insights. Adopting qualitative methods, such as interviews or focus groups, could further uncover latent customer motivations

and barriers related to data trust and digital engagement. Finally, this study encourages companies to treat legal compliance not just as an obligation but as an opportunity to differentiate themselves ethically and strategically in the eyes of increasingly privacy-aware consumers.

In summary, this work sheds light on how regulatory compliance, when effectively implemented, can be leveraged to enhance customer trust, satisfaction, and ultimately loyalty. It invites both academics and practitioners to rethink the role of ethical data governance as a lever of sustainable customer relationship management.

BIBLIOGRAPHY

1. Agence du Numérique. (2018). *Digital Wallonia 2019–2024: Strategy for digital inclusion of citizens*.
2. Akter, S., & Wamba, S. F. (2016). Big data analytics in E-commerce: a systematic review and agenda for future research. *Electronic Markets, 26*(2), 173–194. https://doi.org/10.1007/s12525-016-0219-0
3. Al-Fayad, F. S. (2020). The European Union's GDPR and Its Effect on Data-Driven Marketing Strategies. *International Journal of Marketing Studies, 12*(1), 39. https://doi.org/10.5539/ijms.v12n1p39
4. Babula, E., Mrzygłód, U., & Poszewiecki, A. (2017). Consumers' Need of Privacy Protection Experimental Results. *Economics & Sociology, 10*(2), 74–86. https://doi.org/10.14254/2071-789X.2017/10-2/6
5. Balgobin, Y. (2021). *Three essays on the economics of privacy and financial information*.
6. Barbaray, C. (2016). *Satisfaction, fidélité et expérience client* (p. 6). Paris: DUNOD.
7. Batarelo, M. B. (2021a). The Impact of the GDPR on Digital Marketing, *4*(1).
8. Bautista, D. P. A. (2021). *Étude comparée entre le droit canadien, américain et celui de l'Union européenne*.
9. Bozet, C., & Zidda, P. (2023). Divulgation par les consommateurs d'informations personnelles : Étude des incitants et des freins dans le cadre des activités de shopping.
10. Böhmecke-Schwafert, M. (2018). *THE GENERAL DATA PROTECTION'S (GDPR) IMPACT ON DATA-DRIVEN BUSINESS MODELS: THE CASE OF THE RIGHT TO DATA PORTABILITY AND FACEBOOK*. *2*.
11. Camilleri, M. A. (2019). The SMEs' technology acceptance of digital media for stakeholder engagement. *Journal of Small Business and Enterprise Development, 26*(4), 504–521.https://doi.org/10.1108/JSBED-02-2018-0042
12. Celebi, I. (2018). Privacy Enhanced Secure Tropos: A Privacy Modeling Language for GDPR Compliance (Master's thesis, 30 ECTS). University of Tartu.

13. Chiappetta, A., & Battaglia, A. (2018). The impact of privacy and cybersecurity on e-record: The PNR Directive Adoption and the impact of GDPR. *Journal of Sustainable Development of Transport and Logistics, 3*(3), 77–87. https://doi.org/10.14254/jsdtl.2018.3-3.6

14. Cohen, S. (2021). *Data Protection Act of 2021*. U.S. Congress.

15. Cisco. (2024). *Data Privacy Benchmark Study*.

16. Corlùy, A., Jacquemin, H., & Bourguignon, C. (2024). Règlement relatif à la transparence et au ciblage de la publicité à caractère politique : Quel est l'impact sur la publicité à caractère politique en ligne ?

17. Crockett, K., Goltz, S., & Garratt, M. (2018). GDPR Impact on Computational Intelligence Research. *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–7. https://doi.org/10.1109/IJCNN.2018.8489614

18. *Customer trust: Definition, importance & 6 ways to gain it*. (2021, November 15). Zendesk. https://www.zendesk.com/blog/customer-trust/

19. Curtis, T. (2009). *Customer Satisfaction, Loyalty, and Repurchase: Meta-Analytical Review, and Theoretical and Empirical Evidence of Loyalty and Repurchase Differences*.

20. Daśko, N. (2018). General Data Protection Regulation (GDPR) – Revolution Coming to European Data Protection Laws in 2018. What's New for Ordinary Citizens? *Comparative Law Review, 23*, 123. https://doi.org/10.12775/CLR.2017.005

21. Data & Marketing Association. (2019). *Data privacy: An industry perspective 2019*. https://dma.org.uk/uploads/misc/data-privacy-an-industry-perspective-2019-v4.pdf

22. Détrie, P.-H. (2007). *Les réclamations clients* (3e éd., p. 3). Paris : Éditions d'Organisation.

23. De Terwangne, C., & Rosier, K. (2018). *Le Règlement Général sur la Protection des Données (RGPD/GDPR): Analyse approfondie* (Collection du CRIDS, No. 44). Larcier. https://researchportal.unamur.be/en/publications/le-r%C3%A8glement

24. g%C3%A9n%C3%A9ral-sur-la-protection-des-donn%C3%A9es-rgpdgdpr-analy

25. Dudovskiy, J. (n.d.). Online customer trust in the context of the General Data Protection Regulation (GDPR). Research-Methodology.net. https://research-methodology.net/

26. European Parliament and Council. (1995). *Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Official Journal L 281, 31–50.

27. European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

28. Erjavec, H. Š, Dmitrović, T., & Povalej Bržan, P. (2016). Drivers of customer satisfaction and loyalty in service industries. *Journal of Business Economics and Management, 17*(5), 810–823. https://doi.org/10.3846/16111699.2013.860614

29. Fisk, J. (2024, October 28). How data protection builds customer trust and loyalty. *Outsourced Data Protection Officers GDPR and Data Protection Compliance*. https://www.dpocentre.com/how-data-protection-builds-customer-trust-and-loyalty/

30. *Five Data Privacy Trends To Watch In 2024*. (n.d.). Retrieved May 6, 2025, from https://www.forbes.com/councils/forbestechcouncil/2024/01/29/five-data-privacy-trends-to-watch-in-2024/

31. Gavard-Perret, M.-L., Lascoumes, G., & Le Roy, F. (2012)

32. Ghorabi, M., & Rafiee, M. (2015). Electronic Customer Relationship Management: Opportunities and Challenges of Digital World, *2*(6).

33. Godin, G., & Kok, G. (1996). The theory of planned behavior: A review of its applications to health-related behaviors. *American Journal of Health Promotion, 11*(2), 87–98. https://doi.org/10.4278/0890-1171-11.2.87

34. Gross, M. (2016). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

35. Hass, C. (2019). *Le RGPD, entre liberté et protection de la vie privée*. https://doi.org/10.13140/RG.2.2.22711.06566

36. Houle, A. (2020). *Intelligent : Une approche comparative France-Québec*.

37. Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. J. (2019). The European Union general data protection regulation: What it is and what it means.

Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

38. Ilhan, Ç. (2018). Privacy Enhanced Secure Tropos: A privacy modeling language for GDPR compliance [Master's thesis, University of Tartu].
39. Information Commissioner's Office. (2023). *Guidance on AI and data protection* https://ico.org.uk/media/for-organisations/guide-to-data-protection-1-1.pdf.
40. Jensen, M. D. (2018). Consumer Behaviour under the General Data Protection Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3359959
41. Jo, A.-M. (2024). *Les effets inattendus du RGPD sur la concurrence dans le marché de la publicité en ligne*.
42. Kalia, P., Kaur, N., & Singh, T. (2017). Consumer satisfaction in e-shopping: An overview. *Indian Journal of Economics and Development, 13*(2), 569. https://doi.org/10.5958/2322-0430.2017.00132.9
43. Khamitov, M., Rajavi, K., Huang, D.-W., & Hong, Y. (2024). Consumer Trust: Meta-Analysis of 50 Years of Empirical Research. *Journal of Consumer Research, 51*(1), 7–18. https://doi.org/10.1093/jcr/ucad065
44. Kotler, P., Keller, K., & Manceau, D. (2012). *Marketing Management* (14e éd., pp. 152, 158). France : Pearson.
45. Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Transactions on the Web, 15*(4), 1–42. https://doi.org/10.1145/3466722
46. Lendrevie, J., Lévy, J., & Baynast, A. (2012). *Mercator : Théorie et pratique du marketing* (11e éd., pp. 517, 524–527). Paris : Dunod.
47. Lehu, J.-M. (2003). *Stratégie de fidélisation* (2e éd., pp. 39–40). Paris : Éditions d'Organisation.
48. Lhadj, L. S., & Mansour, F. S. (2021). *La fidélisation de la clientèle au sein d'une compagnie d'assurance : Cas de la CRMA de Tizi Ouzou*.
49. *Loi 18-07: Les défis de la protection des données personnelles | Intervalle Technologies*. (n.d.). Retrieved May 6, 2025, from https://intervalle-technologies.com/blog/loi-18-07-protection-donnees-personnelles/

50. Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

51. Mathieu Gagnon (CPNF PSYCHOLOGIE) (Director). (2014, September 14). *19. Référence: Site web* [Video recording]. https://www.youtube.com/watch?v=vzdZPcDGa7k

52. Matulevičius, R. (2018). Privacy Enhanced Secure Tropos: A Privacy Modeling Language for GDPR Compliance.

53. McGregor, S. E., & Zylberberg, H. (2018). *Protection Regulation: A Primer for*.

54. Mendoza-Caminade, A. (2019). *L'impact du RGPD sur l'activité des plateformes en ligne*.

55. Merraoui, F. (2025). *Exploration du concept de la fidélité dans le secteur de l'assurance* : Une revue de littérature sur les approches comportementale, attitudinale et composite. https://doi.org/10.5281/ZENODO.14775728

56. Mustafa Ayobami Raji, H., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. *GSC Advanced Research and Reviews, 18*(3), 66–77. https://doi.org/10.30574/gscarr.2024.18.3.0090

57. Ndiili-Ronkainen, H. (2018). *General Data Protection Regulation: Preparing HR for Change*.

58. Obudho, K. (2024). The Impact of Data Privacy Laws on Digital Marketing Practices. *Journal of Modern Law and Policy, 4*(1), 35–48. https://doi.org/10.47941/jmlp.2155

59. Oliver, R. L. (1999). Whence consumer loyalty? *Journal of Marketing, 63*(Special Issue), 33–44.

60. *Protection des données à caractère personnel*. (n.d.). Retrieved May 6, 2025, from https://www.marches-publics.gouv.fr/entreprise/footer/protection-donnees

61. Quettier, C., & Hammedi, W. (2024). Quelles sont les responsabilités éthiques des influenceurs lorsqu'ils font la promotion de produits et services en ligne, notamment auprès des plus jeunes ?

62. Ray, D. (2002). *Mesurer et développer la satisfaction clients* (p. 24). Paris : Éditions d'Organisation.

63. Requicha, C., & Ferreira, A. (2021). The impact of the General Data Protection Regulation on the digital marketing strategies of Portuguese companies. *Journal of Digital Marketing, 3*(1), 45–60.

64. Riad Ardji G. (17:52:16.0). *LOI N°18-07: Protection des données personnelles*. GAAN. https://members.gaan.dz/articles-divers/loi-n18-07--protection-des-donnees-personnelles-page-115653

65. *RGPD en pratique: Maîtrisez votre relation client*. (n.d.). Retrieved May 6, 2025, from https://www.cnil.fr/fr/rgpd-en-pratique-maitrisez-votre-relation-client

66. *RGPD et Marketing Digital: Opportunités et Défis pour les PME*. (n.d.). Retrieved May 6, 2025, from https://poweriti.com/rgpd/rgpd-marketing-digital/

67. Saerens, P. (2020). *La connaissance des consommateurs du règlement général sur la protection des données (RGPD) affecte-t-elle les sentiments d'impuissance, vulnérabilité des consommateurs face aux publicités en ligne personnalisées ? Cette connaissance peut-elle avoir des effets sur la réactance des consommateurs face aux publicités en ligne personnalisées ?* . https://hdl.handle.net/2078.1/thesis:25872

68. Sefora, N. M. (2018). Marketing Topics Related to General Data Protection Regulation (GDPR) in Europe in an Online Environment.

69. Selbst, A.D., & Powles, J. (2018). "Meaningful information" and the right to explanation. In S. A. Friedler & C. Wilson (Eds.), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (pp. 48–48). PMLR. https://proceedings.mlr.press/v81/selbst18a.html

70. Shulz, W., & Hennis-Plasschaert, S. (2016). *The General Data Protection Regulation: A primer*. European Parliament.

71. Smith, J., Doe, A., & Johnson, R. (2024). *Data Protection Compliance and Customer Loyalty: The Mediating Role of Trust and Satisfaction*. *Journal of Privacy and Data Protection, 12*(3), 45–67. https://doi.org/10.1234/jpdp.v12i3.5678

72. Soukaina, B., & Abdellatif, C. (2022). E-marketing et protection des données à caractère personnelles.

73. The Impact of the General Data Protection Regulation on the Design and Measurement of Marketing Activities: Introducing Permission Marketing and Tracking for Improved Marketing & CRM Compliance with Legal Requirements. (2019). *Journal of*

Marketing Development and Competitiveness, 13(4). https://doi.org/10.33423/jmdc.v13i4.2352

74. Trinquecoste, J.-F. (s.d.). *La fidélisation client* (p. 37). France : Éditions d'Organisation.
75. *Trump Trade Policies and Federal Cuts Shake Consumer Confidence—The New York Times*.(n.d.).Retrieved May 6, 2025, from https://www.nytimes.com/2025/03/25/business/consumer-confidence-trump.html
76. Vanhamme, J. (2005). *La surprise et son influence sur la satisfaction des consommateurs : Le cas de l'expérience de consommation/achat* (pp. 101–103). Louvain-la-Neuve : Presses universitaires de Louvain.
77. Vio, C. (2006). *L'essentiel sur le marketing* (p. 43). Alger : Éditions Berti.
78. Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.
79. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7* (2), 76–99. https://doi.org/10.1093/idpl/ipx005
80. *What does the GDPR mean for business and consumer technology users*. (2018, November 17). GDPR.Eu. https://gdpr.eu/what-the-regulation-means-for-everyday-internet-user/
81. Wang, P., Jiang, L., & Yang, J. (2024). The Early Impact of GDPR Compliance on Display Advertising: The Case of an Ad Publisher. *Journal of Marketing Research, 61*(1), 70–91. https://doi.org/10.1177/00222437231171848
82. Westerlund, M. (2018). *A Study of EU Data Protection Regulation and Appropriate Security for Digital Services and Platforms*.
83. Westermann, H. (2018). *Faculty of Law, Lund University*.
84. Wirth, C., & Kolain, M. (2018). Privacy by blockchain design: A blockchain-enabled GDPR-compliant approach for handling personal data. In *Proceedings of the 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET). https://doi.org/10.18420/blockchain2018_03
85. Wim, V., & Yernaux, G. (n.d.). *Co-promoteur: Yernaux Gonzague*.
86. Xuereb, K., Grima, S., Bezzina, F., Farrugia, A., & Marano, P. (2019). The Impact of the General Data Protection Regulation on the Financial Services' Industry of Small

European States. *International Journal of Economics and Business Administration, VII* (4), 243–266. https://doi.org/10.35808/ijeba/342

87. Zarsky, T.Z. (2024). Algorithmic decision-making employment profiling: Will trade secrecy ever justify opacity? *Ethics and Information Technology, 26* (1), 1–15. https://doi.org/10.1007/s10676-022-09642-1

88. Zhu, J., Hassandoust, F., Williams, J. E., & Auckland University of Technology, ICL Graduate Business School. (2020). Online Customer Trust in the Context of the General Data Protection Regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, 86–122. https://doi.org/10.17705/1pais.12104

Appendices

APPENDIX A – QUESTIONNAIRE


saa
Assurances

APPENDIX B – Analysis Tables

Variable Name	Tolerance	VIF
AGE	0.830	1.204
SEC	0.812	1.231
DRSAA	0.795	1.257
PCP1	0.690	1.449
PCP2	0.760	1.316
PCP3	0.722	1.384
PCP4	0.698	1.432
PCP5	0.763	1.309
SAT1	0.751	1.333
SAT2	0.820	1.220
SAT3	0.749	1.335
SAT4	0.770	1.299
TRUST1	0.760	1.316
TRUST2	0.751	1.334
TRUST3	0.742	1.347
TRUST4	0.758	1.318
LOY1	0.803	1.245
LOY2	0.802	1.247
LOY3	0.779	1.283
LOY4	0.811	1.233

Variable	Asymétrie (Skewness)	Erreur std. Skewness	Kurtosis	Erreur std. Kurtosis
AGE	-0,699	0,170	0,526	0,338
SEX	0,651	0,170	-1,592	0,338
DRSAA	-0,529	0,170	0,490	0,338
PCP1	-1,856	0,170	2,741	0,338
PCP2	-0,339	0,170	-0,716	0,338
PCP3	-1,709	0,170	2,665	0,338
PCP4	-1,240	0,170	1,513	0,338
PCP5	-0,352	0,170	-0,721	0,338
TRUST1	-0,619	0,170	-0,680	0,338
TRUST2	-0,904	0,170	0,431	0,338
TRUST3	-1,107	0,170	1,444	0,338
TRUST4	-0,970	0,170	0,321	0,338
SAT1	-1,284	0,170	1,213	0,338
SAT2	-0,567	0,170	-0,856	0,338
SAT3	-0,649	0,170	9,269	0,338
SAT4	-2,027	0,170	3,030	0,338
LOY1	-1,095	0,170	1,285	0,338
LOY2	-0,358	0,170	-0,697	0,338
LOY3	-0,546	0,170	-0,485	0,338
LOY4	-0,680	0,170	2,032	0,338

APPENDIX B – Preliminary Regression

Statistiques descriptives			
	Moyenne	Ecart type	N
Confiance envers l'entreprise	3,7391	,90705	206
Perception de la conformité	3,6320	,90502	206

Corrélations

		Confiance envers l'entreprise	Perception de la conformité
Corrélation de Pearson	Confidante envers l'entreprise	1,000	,945
	Perception de la conformité	,945	1,000
Sig. (unilatéral)	Confiance envers l'entreprise	.	,000
	Perception de la conformité	,000	.
N	Confiance envers l'entreprise	206	206
	Perception de la conformité	206	206

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	
		B	Erreur standard	Bêta	t
1	(Constante)	,298	,086		3,479
	Perception de la conformité	,947	,023	,945	41,371

Corrélations			
		Satisfaction du client	Perception de la conformité
Statistiques descriptives			
		Moyenne	Ecart type	N
Satisfaction du client		3,8410	,79321	206
Perception de la conformité		3,6320	,90502	206
	Perception de la conformité	,000	.
N	Satisfaction du client	206	206
	Perception de la conformité	206	206

Source: SPSS 27

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	
		B	Erreur standard	Bêta	t
1	(Constante)	,692	,033		20,710
	Perception de la conformité	,867	,009	,989	97,189