الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratics Republic of Algeria

Ministry of Higher Education
and Scientific Research

National Higher School of Management
University Pole of Kolea

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

GRADUATE DISSERTATION

Submitted in Partial Fulfilment of the Requirements for a Master's Degree in

Electronic Governance

The Role of Data Governance in Personal Data Protection Case Study at SPA Condor Electronics

Submitted by

Mohamed LAHRECHE

Supervised by

Dr. Omar KADI

Academic Year
2025/2026

Abstract

This study investigates how data governance practices at Condor Electronics, one of Algeria's largest private manufacturing conglomerates, contribute to personal data protection, in the context of Law No. 18-07 and its reinforcement through Law No. 25-11, and the near-total absence of empirical research on this subject within the Algerian private sector. A mixed-methods case study design was adopted, combining field observation, documentary analysis of nine ISO 27001:2022-aligned internal policies, and four semi-structured interviews analyzed using NVivo 15, alongside a structured questionnaire administered to 67 IS Division employees and analyzed using SPSS Statistics 31. Qualitative findings revealed that governance practices are operationally present but structurally fragmented, with no unified framework, informally defined roles, a vacant governance manager position since 2023, and a complete absence of data quality management policies. Quantitative analysis confirmed a statistically significant and strong positive effect of data governance on personal data protection, with governance policies and roles emerging as the strongest predictor among all sub-dimensions. The study concludes that data governance at Condor Electronics contributes meaningfully but incompletely to personal data protection, reflecting a low governance maturity profile where practices are positively perceived by employees but operate in an ad hoc manner in the absence of a formal and unified governance framework.

Keywords: Data governance, personal data protection, Law No. 18-07, Condor Electronics, data governance maturity.

Résumé

Ce mémoire examine la contribution des pratiques de gouvernance des données à la protection des données personnelles au sein de Condor Electronics, dans un contexte marqué par l'entrée en vigueur de la loi n° 18-07 et son renforcement par la loi n° 25-11, et par l'absence quasi-totale de recherches empiriques sur ce sujet dans le secteur privé algérien. Une approche mixte a été adoptée, articulant une observation de terrain, une analyse documentaire de neuf politiques internes alignées sur l'ISO 27001:2022, quatre entretiens semi-directifs analysés via NVivo 15, ainsi qu'un questionnaire structuré administré à 67 employés de la direction des systèmes d'information et traité sous SPSS Statistics 31. Les résultats qualitatifs révèlent des pratiques existantes mais fragmentées, sans cadre unifié, avec des rôles informellement définis, un poste de responsable de gouvernance vacant depuis 2023, et une absence totale de politique de gestion de la qualité des données. Les résultats quantitatifs confirment un effet positif et statistiquement significatif de la gouvernance des données sur la protection des données personnelles, la dimension politiques et rôles de gouvernance se distinguant comme le prédicteur le plus fort parmi toutes les sous-dimensions. Ce travail conclut que la gouvernance des données contribue de manière réelle mais incomplète à la protection des données personnelles à Condor Electronics, reflétant un profil de maturité faible où les pratiques existent mais fonctionnent de manière ad hoc en l'absence d'un cadre formalisé.

Mots-clés: Gouvernance des données, protection des données personnelles, loi n° 18-07, Condor Electronics, maturité de la gouvernance des données.

الملخص

تهدف الدراسة إلى تشخيص واقع تطبيق حوكمة البيانات في مؤسسة كوندور للإلكترونيات، وقياس أثرها على حماية البيانات الشخصية، واستخلاص توصيات عملية تُمكّن المؤسسة من تعزيز بنيتها الحوكمية وفق ما تقتضيه المنظومة التشريعية النافذة. وتتناول الدراسة مسألة مساهمة ممارسات حوكمة البيانات في حماية البيانات الشخصية بالمؤسسة، في ظل ما أفرزه القانون رقم 18-07 المعزَّز بالقانون رقم 25-11 من التزامات مُلزِمة، وما يتسم به المشهد الأكاديمي الجزائري من شُح ملحوظ في الدراسات الميدانية المتعلقة بهذا الموضوع. اعتمدت الدراسة منهجاً بحثياً مختلطاً يقوم على الملاحظة الميدانية، وتحليل تسع وثائق سياسات داخلية وفق معيار ISO 27001:2022، وأربع مقابلات شبه موجهة حُلِّلت عبر NVivo 15، إضافة إلى استبيان منظم وُزّع على 67 موظفاً من قسم نظم المعلومات وعولجت بياناته ببرنامج SPSS Statistics 31. كشفت النتائج النوعية أن ممارسات الحوكمة قائمة على أرض الواقع غير أنها مجزأة وتفتقر إلى إطار موحد، في ظل غياب تام لسياسة إدارة جودة البيانات وعدم رسمية الأدوار الحوكمية. وأثبتت النتائج الكمية وجود أثر إيجابي ودال إحصائياً لحوكمة البيانات على حماية البيانات الشخصية، إذ تصدّرت بُعد السياسات وأدوار الحوكمة قائمة المتنبئات من بين جميع الأبعاد الفرعية. وتخلص الدراسة إلى أن حوكمة البيانات تُسهم إسهاماً حقيقياً لكن غير مكتمل في حماية البيانات الشخصية بمؤسسة كوندور، في ظل مستوى نضج حوكمي منخفض تعمل فيه الممارسات بصورة غير منهجية بعيداً عن أي إطار رسمي وموحد.

الكلمات المفتاحية: حوكمة البيانات، حماية البيانات الشخصية، القانون رقم 18-07، كوندور للإلكترونيات، نضج حوكمة البيانات.

Acknowledgments

First and foremost, all praise and gratitude are due to Allah, the Most Gracious, the Most Merciful. Without His divine guidance and blessings, none of this would have been possible.

I extend my deepest thanks to all those who have supported me throughout this journey. To my tutors and professors, whose wisdom and dedication have shaped my understanding, I am sincerely grateful. I am especially thankful to **Mr. Omar KADI**, whose guidance and encouragement as my academic supervisor were invaluable throughout the development of this work.

A special word of thanks is also extended to **Rami SAIDOUNI**, with heartfelt appreciation, for introducing me to the Higher National School of Management (ENSM) and encouraging me to pursue my studies here, a decision that has proven deeply rewarding.

I am equally indebted to **Mr. Elyes MATOUG**, my internship tutor at Condor Electronics, whose generosity, patience, and unwavering readiness to assist enriched my experience beyond words. His guidance was a steady compass throughout this project.

My heartfelt appreciation also goes to my family, my parents, who stood by me with unconditional love and strength, and my friends, old and new. To those companions who walked beside me over the past two years, who laughed with me, worked late with me, and made this school feel like a second home, I thank you deeply. These memories shall forever remain etched in my heart.

This work is not merely the result of my own efforts but a reflection of the care, wisdom, and kindness of many. To all who have contributed, directly or silently, I am eternally grateful.

Mohamed L.

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

Abbreviations

ACS	Access Control and Security
AI	Artificial Intelligence
ANOVA	Analysis of Variance
ANPDP	*Autorité Nationale de Protection des Données à Caractère Personnel* (National Authority for the Protection of Personal Data)
BPO	Business Process Owner
BU	Business Unit
CAQDAS	Computer-Assisted Qualitative Data Analysis Software
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
COVID-19	Coronavirus Disease 2019
DaLiF	Data Lifecycle Framework
DAMA	Data Management Association International
DBA	Database Administrator
DCAM	Data Management Capability Assessment Model
DDoS	Distributed Denial-of-Service
DG	Data Governance
DLM	Data Lifecycle Management
DMBOK	Data Management Body of Knowledge
DPO	Data Protection Officer
DQM	Data Quality Management
DSI	*Directeur des Systèmes information* (Director of Information Systems)
EDPB	European Data Protection Board
EU	European Union
FGD	Focus Group Discussion
GDPR	General Data Protection Regulation
GLPI	*Gestionnaire Libre de Parc Informatique* (IT asset/ticketing platform)
GPR	Governance Policies and Roles
HIPAA	Health Insurance Portability and Accountability Act (US)
HMS	Hospital Management Systems

HR	Human Resources
HVAC	Heating, Ventilation, and Air Conditioning
IBM	International Business Machines Corporation
IEC	International Electrotechnical Commission
IOC	Item-Objective Congruence
IoT	Internet of Things
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
LCM	Liquid Crystal Module
LGPD	*Lei Geral de Proteção de Dados* (Brazilian General Data Protection Law)
MDM	Master Data Management
MFA	Multi-Factor Authentication
NDA	Non-Disclosure Agreement
PAM	Privileged Access Management
PDP	Personal Data Protection
QHSE	Quality, Health, Safety, and Environment
QR	Quick Response (QR code)
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAP	Systems, Applications, and Products in Data Processing
SLR	Systematic Literature Review
SMPC	Secure Multi-Party Computation
SPA	*Société par action* (Joint-stock company)
SPBE	*Sistem Pemerintahan Berbasis Elektronik* (Electronic-Based Government Systems)
SPSS	Statistical Package for the Social Sciences
SSOT	Single Source of Truth
UAE	United Arab Emirates
US	United States
USB	Universal Serial Bus
VIF	Variance Inflation Factor

Symbols

α	Cronbach's alpha coefficient (reliability); also used as significance threshold (α = 0.05)
β / Beta	Standardized regression coefficient (Beta)
B	Unstandardized regression coefficient
df	Degrees of freedom
F	F-statistic (ANOVA / regression significance test)
H_0	Null hypothesis
H_1	Alternative hypothesis
M	Mean (arithmetic average)
n	Sample size
p	Probability value (significance level)
r	Pearson correlation coefficient
R	Multiple correlation coefficient
R^2	Coefficient of determination (proportion of variance explained)
Adj. R^2	Adjusted coefficient of determination
SD	Standard deviation
Sig.	Significance (p-value as reported in SPSS output)
t	t-statistic (from t-test or regression coefficients table)
W	Shapiro-Wilk test statistic
y	Predicted value in regression equation (dependent variable)
x	Predictor variable in regression equation (independent variable)

GENERAL INTRODUCTION

Data has become one of the most critical assets organizations manage, while simultaneously representing a growing source of risk if left ungoverned. The spread of advanced technologies, including the internet and artificial intelligence, has led to increased collection and exchange of personal data, exposing it to mounting risks related to privacy and security, and prompting countries worldwide to adopt legislation regulating its processing in line with international standards (Imad, 2024).

Data governance has emerged as a central organizational response to these challenges. It refers to the exercise of authority and control over the management of data, with the core purpose of increasing its value while minimizing data-related cost and risk (Abraham et al., 2019). A governance framework provides a structured approach to managing data within an organization, ensuring that it is protected from internal and external threats, complies with legal and regulatory standards, and is used in an ethical and responsible manner (Julakanti et al., 2025).

Algeria has engaged with this global dynamic through a developing legislative framework. Law No. 18-07 of June 10, 2018 established the national framework for the protection of personal data and created the National Authority for the Protection of Personal Data (ANPDP). Law No. 25-11 of 2025 reinforced these provisions by introducing obligations such as the mandatory appointment of a Data Protection Officer and the conduct of Data Protection Impact Assessments.

It is within this context that the present study examines how data governance practices at Condor Electronics contribute to personal data protection.

- **Rationale for Choosing the Topic**

The choice of this research topic is motivated by four converging considerations. First, academic literature examining data governance within the Algerian context is exceptionally scarce, leaving a significant gap that the present study seeks to address. Second, its relationship with personal data protection outcomes at the firm level remains empirically underexplored, particularly outside European regulatory contexts. Third, Algeria's evolving legal framework has created binding obligations that Algerian enterprises have not yet been empirically studied against. Fourth, Condor Electronics, as one of Algeria's largest private manufacturing conglomerates, constitutes a representative and accessible site for this inquiry. These four factors together justify the focus and title of the present study.

- **Research Problem and Questions**

Despite its growing importance in organizational practice, a holistic view on data governance that could guide both practitioners and researchers has remained largely absent from the literature (Abraham et al., 2019). At the same time, the proliferation of personal data generated by digital systems has made its protection a matter of both legal obligation and organizational responsibility. The concept of data governance is not new, but its importance has been magnified by the rapid digitalization and an increasingly demanding regulatory environment, as governments around the world enact stringent data protection regulations to hold organizations accountable for how they collect, store, and process personal information (Julakanti et al., 2025).

Regulatory and legal frameworks, though present, are frequently not enforced, demonstrating a persistent gap between legislation and implementation, with limited awareness and capacity representing deep structural barriers to compliance at the organizational level (Masinde et al., 2025). Despite Algeria's legal advancements, the practical application of these laws still faces significant challenges that require continuous efforts to ensure full compliance and address legal gaps (Imad, 2024). Algeria established a legal framework for data privacy through Law No. 18-07, enacted on June 10, 2018, and officially came into force on August 10, 2023 (Law No. 18-07, 2018), before further strengthening it through Law No. 25-11, which introduced obligations including the mandatory appointment of a Data Protection Officer and the conduct of Data Protection Impact Assessments (Law No. 25-11, 2025). It is within this context that the present study is situated, leading to the following central question:

How does data governance, as delivered by its practices at Condor Electronics, contribute towards personal data protection?

From this central question, four sub-questions are derived:

1. To what extent does Condor implement data governance practices?
2. How does Condor handle personal data breaches and incidents?
3. To what extent do Condor's employees comply with personal data protection policies and practices?
4. What challenges does Condor face in protecting personal data, and how can data governance practices help overcome these challenges?

- **Research Hypotheses**

In response to the central research problem, and in order to guide the quantitative strand of the study, the following main hypothesis is proposed: data governance practices have a statistically significant positive effect on personal data protection at Condor Electronics (H_1), against the null hypothesis that no such effect exists (H_0). This main hypothesis is further decomposed into four sub-hypotheses corresponding to each of the four data governance dimensions examined in this study:

- **H_1a:** Data quality management has a statistically significant positive effect on personal data protection.
- **H_1b:** Access control and security has a statistically significant positive effect on personal data protection.
- **H_1c:** Data lifecycle management has a statistically significant positive effect on personal data protection.
- **H_1d:** Governance policies and roles has a statistically significant positive effect on personal data protection.

Each sub-hypothesis carries a corresponding null hypothesis stating that the respective dimension has no statistically significant effect on personal data protection.

- **Goals of the Study**

This study pursues three interconnected objectives:

1. **Descriptive:** To examine and document the extent to which data governance practices are currently implemented within the Information Systems Division of Condor Electronics, across the four dimensions of data quality management, access control and security, data lifecycle management, and governance policies and roles.
2. **Analytical:** To investigate the relationship between these governance practices and personal data protection outcomes, specifically whether variation in governance implementation is associated with variation in protection outcomes as perceived by IS division employees.
3. **Applied:** To derive practical recommendations enabling Condor Electronics to strengthen its data governance architecture in alignment with Laws No. 18-07 and No. 25-11, while contributing empirical evidence to the literature on data governance and personal data protection in Algerian private sector organizations.

- **Significance of the Study**

This study carries significance at three levels: academic, institutional, and regulatory.

At the academic level, by empirically examining the relationship between data governance practices and personal data protection outcomes within a private sector manufacturing organization, this study produces firm-level evidence of a kind that the existing literature has not yet generated for the Algerian context. The mixed-methods design further allows quantitative patterns to be grounded in qualitative organizational reality, producing a richer and more transferable contribution than either approach alone could yield.

At the institutional level, the findings offer Condor Electronics a clearer picture of its data governance maturity and its implications for personal data protection outcomes. At a moment when the ANPDP has extended its field inspection activities to private sector organizations, the study's practical recommendations offer the organization concrete pathways toward strengthening its governance architecture in alignment with its existing legal obligations.

At the regulatory level, by documenting how a private Algerian organization operationalizes data protection governance under Laws No. 18-07 and No. 25-11, this study provides policymakers and practitioners with grounded evidence of where implementation gaps persist and where compliance efforts are taking hold. This kind of case-based organizational evidence is currently absent from the Algerian regulatory discourse and carries direct relevance for the ANPDP's ongoing enforcement and capacity-building efforts.

- **Methodology**

This study is grounded in a pragmatist epistemological stance, prioritizing research questions over methodological purity and treating both qualitative and quantitative forms of knowledge as valid insofar as they contribute to understanding the research problem, providing the philosophical justification for the mixed-methods case study design adopted.

The qualitative strand encompasses field observation analyzed through thematic analysis, documentary analysis of nine ISO 27001:2022-aligned policy documents examined through content analysis, and four semi-structured interviews with key informants, namely the Chief Information Security Officer, the IS Project Engineer, the Legal Officer, and the Human Resources Officer, analyzed through a lexical approach, a linguistic approach, cognitive mapping, and thematic analysis using NVivo 15.

The quantitative strand consists of a structured questionnaire administered to the full IS division population, yielding 67 valid responses. It measures data governance across four dimensions and personal data protection as a dependent variable, across 30 Likert-scale items, with statistical analysis performed using SPSS Statistics 31, including Cronbach's alpha, descriptive statistics, regression, and Pearson correlation. Triangulation across both strands was used to produce convergent and contextually grounded conclusions.

- **Structure of the Dissertation**

This dissertation is organized into three chapters in addition to this general introduction and a general conclusion.

Chapter I establishes the theoretical and conceptual framework of the study. It is divided into two sections. The first section presents a systematic review of the literature on data governance, personal data protection, and the relationship between the two domains, concluding with a comparative summary of prior studies that identifies the thematic gaps this research addresses. The second section develops the conceptual framework, covering the definition, pillars, frameworks, and maturity models of data governance, and the legal framework of personal data protection in Algeria under Laws No. 18-07 and No. 25-11, including their key definitions, fundamental principles, obligations, sanctions, and implementation challenges.

Chapter II presents the data and methods underpinning the study. It opens with an overview of Condor Electronics as the case study organization, before detailing the philosophical underpinnings of the research design, the rationale for the mixed-methods case study approach, the data collection instruments and procedures, and the analytical methods applied to both the qualitative and quantitative data.

Chapter III presents and discusses the empirical findings. Drawing on the full body of evidence collected through field observation, documentary analysis, semi-structured interviews, and the administered questionnaire, it first presents and analyzes the qualitative and quantitative results in turn, before discussing them through triangulation across all data sources to address each of the four research questions and the central problematic, situate the findings within the existing literature, and derive practical and theoretical implications from the results.

CHAPTER I

THEORETICAL FRAMEWORK

This chapter establishes the theoretical foundation for the study, which investigates the role of data governance in shaping personal data protection outcomes within the Algerian private sector, using Condor Electronics as a case study. The chapter is divided into two main sections. The first section presents a comprehensive literature review, synthesizing existing research on data governance, personal data protection, and their interrelationship. It concludes with a comparative summary of prior studies to identify key thematic gaps that this research aims to address. The second section develops the conceptual framework, defining the core concepts and pillars of data governance and detailing the regulatory landscape of personal data protection in Algeria under Laws No. 18-07 and No. 25-11. Together, these sections provide the necessary background and analytical lens for the empirical investigation that follows.

Section 1: Literature Review

This section reviews the literature on data governance, personal data protection, and their interrelationship. This review integrates the main theoretical and regulatory views and points out implementation issues and gaps in the existing research. The section concludes with a comparative summary of prior studies to highlight key thematic gaps, thereby positioning the current study.

1. Data Governance

According to Alhassan et al. (2016) Data governance is defined as "A companywide framework for assigning decision-related rights and duties in order to be able to adequately handle data as a company asset" (p. 65), although there is no single universal definition and meanings vary across sectors and professional communities. Gupta & Cannon (2020) note that definitions can be more or less specific and emphatic, and the semantic expression is dependent on organizational culture, and some of them can be more control-oriented or prescription-oriented.

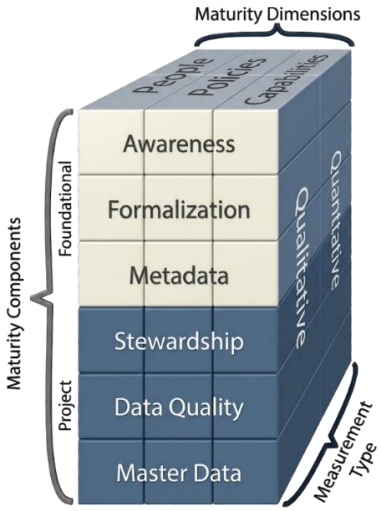
Expanding on this perspective, Koltay (2016) directly mentions that the solution to the problem of data quality in research settings is the data governance that defines clear decision rights, policies, and accountability structures. His study demonstrates that data governance and data literacy are closely related and affect effective data management and decision-making, and governance framework implementation increases transparency and efficiency. Koltay further argues that data literacy competencies among professionals should be enhanced to maximize benefits of governance practices.

Reflecting this emphasis on structured approaches, Smith (2023) underscores that detailed data governance plans are essential to ensure data integrity. On the example of effective governance, the author describes that data quality management, lifecycle control, and data stewardship are coordinated practices that must be used to guarantee reliability. It is also highlighted in the study that technological tools and organizational policies can be used to support these processes, which further confirms that strong governance systems are significant to support compliant and trustworthy data environments.

Building on the discussion of structured practices, Dutta (2016) suggests that property graph-based models for governing real-time data ingestion in industrial Data Lakes resolve challenges of high-speed unstructured data from various sources. This architecture allows stakeholders to visualize and manage governance metadata using graph databases, which perform better than conventional relational systems. Experiments prove that graph-based governance provides constant-time query patterns regardless of data scales, effectively overcoming big data challenges of quality, security, and compliance.

Turning to the assessment of governance capabilities, Wulandari (2020) used the Stanford Data Governance Maturity Model at the National Archives of Indonesia and found a maturity level of 1.35 (initial level) on both foundational and project levels. Analysis reveals that data governance requires continuous refinement of people, policies, and capabilities to meet external regulatory forces like electronic-based government systems. The study highlights the importance of developing competencies over time using structured models such as DMBOK.

Figure 01: Stanford Data Governance Maturity Model



Source: Prepared by the author based on Wulandari (2020).

Complementing the focus on maturity, Chukwurah et al. (2024) discuss the multitude of challenges that organizations can face when developing the data governance frameworks in a recent contribution. These barriers cut across organizational impediments such as the lack of leadership support, data silos, and change resistance. They also outline a set of strategic actions that organizations can embrace to mitigate such challenges. These include the establishment of sound executive sponsorship, and the definition of clear roles and responsibilities, the establishment of strict data quality and security mechanisms.

Similarly, Hikmawati et al. (2021) state that Master Data Management (MDM) is a key component of data governance since it consolidates master data in distributed systems to ensure consistency and accuracy. Their literature review demonstrates that MDM faces data quality challenges including duplication and ambiguity by data profiling, data consolidation, and data cleansing. Moreover, MDM defines explicit roles for business and IT stakeholders in governance mechanisms, ensuring high quality master data as a strategic resource that supports informed decision-making across the organization.

Finally, extending the discussion beyond technical and organizational barriers, the universal requirement of a culturally sensitive approach is presented by Griffiths et al. (2021) who state that the structure of data governance should reflect the cultural requirements of the community it serves, particularly with the Indigenous population, in which the traditional data governance structures should be respected and integrated into the wider scope of healthcare data management.

Overall, the literature on data governance converges on an enterprise-wide framework of roles, policies and decision rights, but studies emphasize control, quality, literacy or technology according to context (Alhassan et al., 2016; Gupta & Cannon, 2020; Koltay, 2016). Quality and literacy focused studies (Hikmawati et al., 2021; Koltay, 2016; Smith, 2023) remain largely generic or research-sector oriented and do not examine alignment with personal data obligations in commercial environments. Technology-oriented contributions (Dutta, 2016) and MDM approaches (Hikmawati et al., 2021) are more concerned with performance than encoding legal responsibilities like consent or retention into governance artefacts. Low maturity and barriers are emphasized in maturity studies (Chukwurah et al., 2024; Griffiths et al., 2021; Wulandari, 2020) but seldom are systematically related to the national data protection regimes, creating a gap in understanding how data governance

practices are implemented in private sector contexts such as Condor within the Algerian regulatory landscape.

2. Personal Data Protection

Al Khatib et al. (2024) highlight the difficulty of introducing General Data Protection Regulation (GDPR) compliance into healthcare information systems, especially where unified regulatory systems are absent. The authors outline that privacy by design, consent management, and data protection impact assessments are essential governance mechanisms for achieving patient data security and regulatory adherence. They also identify cross-border data transfer and third-party management as requiring more explicit laws and organizational activities.

Extending the discussion of legal frameworks, Benamrane et al. (2025) examine the specific rights granted to individuals under Algerian Law No. 18-07, including rights to information, access, rectification, and objection to direct marketing, as essential mechanisms for preserving personal autonomy against artificial intelligence threats. The authors analyze how these legal protections, alongside obligations imposed on data controllers regarding confidentiality and data integrity, form the foundation for safeguarding privacy in an era of increasingly autonomous technological processes.

Justyna & Eva (2020) demonstrate that the importance of personal data protection as a competitive advantage strategy for businesses has also received considerable scholarly attention. The authors demonstrate that data security is gradually viewed as an extension of product quality and customer service. They discovered that despite client and staff awareness, the absence of communication and knowledge among employees frequently leads to inadvertent errors, and that effective data protection can increase customer trust and act as market differentiation.

In this regard, Spalević & Vićentijević (2022) cover the problem of implementing GDPR in the EU and candidate countries like Serbia. Their study summarized key approaches in the GDPR, such as better individual rights, higher transparency requirements, and severe penalty provisions. According to their discussion, synchronizing of national laws with European laws would demand a lot of organizational modification, technical solutions and enforcement of by-laws to guarantee total compliance.

According to Abdelli (2020), the cross-border data flows imply the necessity to align national regulations with international standards. The author focuses on the Law No. 18-07

on personal data protection in Algeria that created the National Authority for the Protection of Personal Data (ANPDP). Abdelli observes that the lack of proper protection criteria in recipient nations leaves the data subjects and supervisory authorities unaware of information transfers across borders therefore requiring regulation by legal means like Convention 108, the treaty on data protection of the Council of Europe.

Shifting focus to technical implementations, Mishra (2024) suggests the framework that relies on the principles of differential privacy, secure multi-party computation, and homomorphic encryption to enable data sharing in healthcare and ensure safety and adherence to Health Insurance Portability and Accountability Act (HIPAA) and GDPR. The author uses experimental validation to show that data perturbation and encryption can be used to exclude unauthorized access and preserve data utility to be used in research.

Within this technical context, Zanke & Sontakke (2024) indicate that telemedicine has some data protection issues that should be subject to strict regulations. Expanding on this, Williamson & Prybutok (2024) shed light on the ethical trade-off that should be obtained in the use of AI in healthcare, such as patient autonomy and data integrity. At a larger level, Ramadhan et al. (2024) discuss the necessity of enacting some laws concerning the security of personal data in the state where the AI technology is developing fast, and this is what has happened in Indonesia.

Beyond healthcare, Cveticanin et al. (2023) observe that new technologies like autonomous vehicles are posing an even greater threat to privacy and the security of personal data. The authors state that autonomous vehicles need a lot of personal data that may create cybersecurity risks and regulatory loopholes. Their findings show that individuals do not trust because of the fear of inadequate data security, and it is important to formulate holistic regulations to strike a balance between innovation and personal rights.

Extending the comparative legal analysis to South Asia, Ali & Hussain (2024) offer a comparative account of data protection law in India and Pakistan, comparing India's Digital Personal Data Protection Act (2023) with Pakistan's proposed Personal Data Protection Bill (2023). Their comparison identifies similarities and differences in frameworks regulating consent, data subject rights, and enforcement mechanisms, while identifying weaknesses in both legislative approaches.

Taken together, the previous studies on the protection of personal data are largely legal and industry-specific, outlining the regulatory requirements but not the alignment of firms to

governance systems. The principles of lawfulness and data subject rights are discussed in GDPR and national legislation studies (Ali & Ahmad Hussain, 2024; Ramadhan et al., 2024; Spalević & Vićentijević, 2022), whereas the provisions of the Law No. 18-07 are described in Algerian studies (Abdelli, 2020; Benamrane et al., 2025), but these works are mostly doctrinal. Privacy by design and technologies are shown in sectoral contributions in healthcare, AI, and emerging technologies (Al Khatib et al., 2024; Cveticanin et al., 2023; Mishra, 2024; Zanke & Sontakke, 2024) but are not focused on the electronics manufacturing industry. Protection is viewed through the prism of business-oriented work (Justyna & Eva, 2020) and concentrates on perceptions rather than internal governance mechanisms. This case study aims to bridge this gap by analyzing how Condor translates the requirements of Laws No. 18-07 and No. 25-11 into concrete policies, roles, and systems.

3. The Relationship between Data Governance and Personal Data Protection

Julakanti et al., (2025) highlight that the connection between data protection and data governance is emphasized in the literature, since data governance frameworks offer the structural framework on which sensitive information protection is provided. The authors state that data governance frameworks comprise policies, roles, and mechanisms that aid in risk management, access control, and regulatory compliance. They observe that security incidents are curtailed by effective governance mechanisms and compliance is enhanced, confirming that data protection is achievable through data governance.

Extending this line of reasoning, data governance and personal data protection are inseparable, as effective implementation of personal data protection is incomplete without a robust data governance structure, a relationship formalized in the proposed Personal Data Protection Integrated Data Governance Management System, which integrates a governance management system with a set of controls to address personal data risks across the entire data lifecycle (Ketmaneechairat et al., 2024).

Turning to empirical evidence, Ferrão et al. (2021) discovered that most Brazilian organizations were not mature in terms of governance and data management. In their survey, they discovered that only 16 per cent had a methodology to test compliance on data protection, and more than 40 percent were not aware of whether there were privacy-impact reports they were required to have.

Further highlighting this complexity, Elgujja et al. (2024) demonstrate that data governance structures establish regulations of the management of personal data, yet without a comprehensive data-protection law, they do not have the force of law. Based on the example of interim regulations in Saudi Arabia, the authors reveal that there should be certain data-protection laws that support the mechanisms of governance to create meaningful and enforceable accountability.

Shah et al. (2021) bring these threads together, illustrating that the integration of data governance and protection is essential to data management. This is demonstrated in their DaLiF framework, where data governance is applied throughout the entire data lifecycle to support data quality, security, and privacy in government big-data environments.

Overall, the literature that directly correlates data governance and personal data protection suggests that governance can be used as the structural foundation of compliance but does not investigate this empirically in non-EU private sector settings. The protection requirements can be embedded in the governance structures (Julakanti et al., 2025; Shah et al., 2021), and integrated models (Ketmaneechairat et al., 2024) suggest combined systems throughout the data lifecycle. Low governance maturity and a lack of alignment between regulations and binding law are found in empirical studies (Elgujja et al., 2024; Ferrão et al., 2021) but are found in Brazil, Saudi Arabia or governmental ecosystems. The scarcity of firm-level analyses under Laws No. 18-07 and No. 25-11 means the concrete ways governance arrangements support personal data protection in Algerian companies remain underexplored, creating a clear niche for this study.

Table 01: Comparative Summary of Reviewed Studies

Prior Study (Author, Year)	***Study Scope***	***Methodology***	***Limitations***
Abdelli, 2020	Algerian Law No. 18-07 and cross-border data flows	Legal/policy analysis	National legal focus; lacks firm-level implementation evidence
Al Khatib et al., 2024	GDPR compliance issues in HMS (UAE healthcare)	Systematic literature review	Sector-specific (healthcare) and jurisdiction-specific (UAE/GDPR)
Alhassan et al., 2016	Data governance activities across literature	Literature synthesis	No testing of DG effects on PDP outcomes in industrial firm; lacks Algeria context
Ali & Hussain, 2024	Data protection legislation (India vs Pakistan)	Comparative legal investigation	Macro-legal compared to micro-DG implementation; not Algeria/industrial

Benamrane et al., 2025	PDP in AI age; Algeria's Law No. 18-07 enforcement	Legal/policy discussion	Limited firm-level DG operations evidence on how private companies implement DG structures
Chukwurah et al., 2024	DG frameworks/best practices across industries	Review synthesis	Broad; lacks single-firm PDP links
Cveticanin et al., 2023	Self-driving cars privacy/security framework	Quantitative approach (questionnaire)	Autonomous vehicles compared to enterprise IS governance
Dutta, 2016	Graph-based architecture for industrial data lakes	Conceptual model	No empirical PDP compliance testing
Elgujja et al., 2024	COVID-19 apps for health surveillance	Literature/legal analysis	Crisis context compared to routine industrial
Ferrão et al., 2021	Brazilian LGPD compliance perceptions	Quantitative approach (Survey diagnostic)	Survey gaps; no firm process-tracing
Griffiths et al., 2021	Indigenous health data governance	Systematic review	Health research; lacks industrial DG
Gupta & Cannon, 2020	DG definitions across sectors	Literature review	Definitional; no operational PDP case
Hikmawati et al., 2021	MDM for data quality/governance	Literature review	No empirical PDP support demonstration
Julakanti et al., 2025	Data protection governance frameworks	Mixed approach (qualitative/ quantitative)	Cross-sector synthesis lacks single-firm depth in Algerian industry
Justyna & Eva, 2020	Personal data protection as competitive advantage	Survey-based empirical study	Enterprise-level survey; lacks detailed governance mechanism analysis
Ketmaneechairat et al., 2024	Integration of PDP and DG management system framework (Thailand)	Framework development with expert validation (IOC) and survey	Thai legal context; framework proposed but not empirically tested in industrial firms
Koltay, 2016	DG, literacy, quality links	Conceptual discussion	No industrial implementation
Mishra, 2024	Healthcare data-sharing platform	Analysis, case studies, and empirical assessments	Technical; limited governance focus. Healthcare-specific with global standards (HIPAA/GDPR)
Ramadhan et al., 2024	Indonesian PDP/AI regulation	Normative legal research	No industrial implementation
Shah et al., 2021	Governance lifecycle models/DaLiF	Systematic review	Public sector; untested in industry
Smith, 2023	Data governance strategies for data integrity	Conceptual framework with case study illustration	Framework presented conceptually; lacks empirical validation of PDP integration in industrial contexts

Spalević & Vićentijević, 2022	GDPR implementation challenges in EU/Serbia	Legal/policy analysis	Regulatory compliance focus; lacks firm-level governance operationalization
Williamson & Prybutok, 2024	Privacy challenges in AI-driven healthcare	Systematic literature review	Healthcare/AI focus; technical privacy-preserving methods not linked to organizational governance structures
Wulandari et al., 2020	Data governance maturity assessment in Indonesian National Archives	Case study using Stanford Maturity Model and FGD with IT/archival unit	Limited to single government unit (Pusdatin); sector-specific (government archives); not industrial/manufacturing context
Zanke & Sontakke, 2024	Telemedicine data protection	Systematic literature review	Telemedicine-specific; no industrial application

Source: Prepared by the author based on previous studies.

In conclusion, the three axes collectively demonstrate that existing literature recognizes data governance as essential for data quality and risk management and personal data protection as grounded in evolving legal and technical frameworks, yet it provides limited empirical insight into how these domains interact in Algerian private sector organizations subject to Laws No. 18-07 and No. 25-11. The literature is fragmented across disciplines and sectors and largely conceptual or legal in nature, and by using a mixed methods case study of Condor Electronics, the study adds value by empirically examining how the role of data governance shapes personal data protection outcomes, clarifying the operational links between governance and protection in a national and sectoral context that current research has largely overlooked.

Section 2: Conceptual Framework

This section outlines the conceptual framework underpinning the current study and specifically, data governance and personal data protection. For data governance, the discussion covers its definition, importance, foundational pillars, and relevant frameworks and maturity models. For personal data protection, the section addresses its definition, the regulatory context under Laws No. 18-07 and No. 25-11, and the main challenges faced in implementation.

1. Data Governance

Data is not a commodity but a capital asset, driving businesses, generating value, and providing a competitive edge when managed and trusted appropriately. Similar to financial assets, it requires careful handling, quality control, security, and ongoing maintenance over

time. This necessity gives rise to data governance: the establishment and implementation of policies and standards to ensure that data is treated with care, responsibility, and legal compliance throughout the enterprise (Petrella, 2020).

1.1. Definition of Data Governance

To begin with, data governance can be introduced through a simple and foundational definition. As Gupta (2020) states, “Data Governance is a collection of practices and processes which help to ensure the formal management of data assets within an organization” (p. 11).

Building on this foundation, Microsoft (n.d.-a) provides a more detailed explanation by stating, “The definition of data governance includes the collection of processes, policies, roles, metrics, and standards that ensure an effective and efficient use of information. This also helps establish data management processes that keep your data secured, private, accurate, and usable throughout the data life cycle” ("Data Governance Definition" section).

Similarly, Maffeo (2023) broadens the scope by highlighting scale and standardization, explaining that “Data governance is a multidisciplinary approach to making and upholding standards that manage data at scale. It helps organizations assess data sourcing, quality, and security at all stages of the data pipeline, from receiving the first spreadsheets with raw data to monitoring that data’s quality once it’s in production” (p. 24).

Moving toward a lifecycle-oriented perspective, McDowall (2019) defines data governance as “the sum total of arrangements to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle” (p. 89).

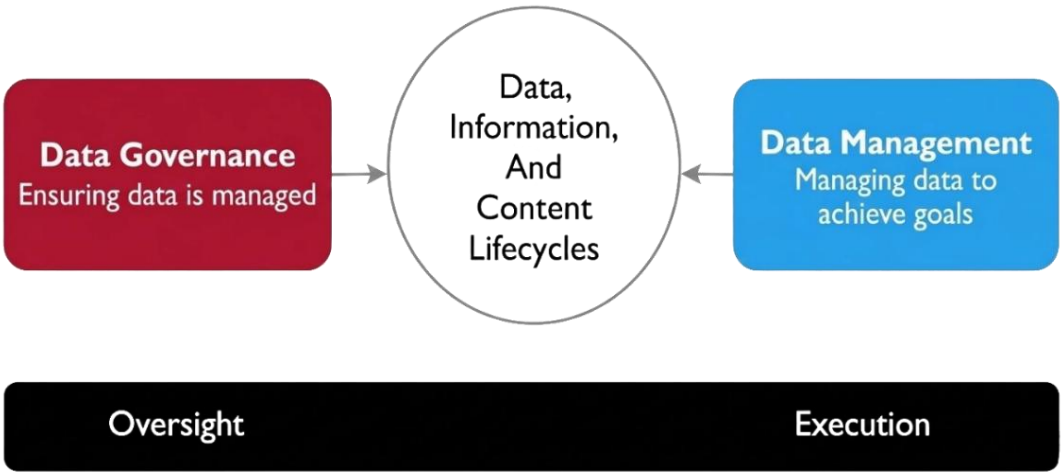
Expanding the scope further, a foundational industry definition comes from DAMA International (2017), the leading global association for data management professionals, which defines data governance as “the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets. All organizations make decisions about data, regardless of whether they have a formal data governance function. Those that establish a formal data governance program exercise authority and control with greater intentionality. Such organizations are better able to increase the value they get from their data assets” (p. 67).

Moving from authority to accountability, Mahanti (2021a) introduces the dimension of enforcement and responsibility, defining data governance as “exercise and enforcement of rules, processes, policies, practices, standards, controls, decision rights, and people accountabilities to manage data as a strategic enterprise asset” (p. 97).

Finally, elevating the concept to its most comprehensive organizational perspective, Batchelder (2024) explains that “Data governance is the formal orchestration of people, processes, and technology by which an organization brings together the right data at the right time with the right controls to enable the company to drive efficient and effective business results. This formal orchestration should control, protect, deliver, and further enhance the value of data and create equity for an organization” (p. 46).

Reflecting on these definitions, it is essential to distinguish data governance from data management. As illustrated in Figure 02, data governance provides oversight, authority, and control, ensuring data is properly managed without directly executing the operational tasks of data management. This separation of duty between governance and execution is fundamental to understanding how organizations structure their data-related responsibilities (DAMA International, 2017).

Figure 02: Data Governance and Data Management



Source: Prepared by the author based on DAMA International (2017).

1.2. Importance of Data Governance in Organizations

According to Eryurek et al. (2021), an effective data governance plan paired with a solid operating model empowers organizations to control their data resources, delivering a competitive edge through:

- Better decision-making, as improved data discoverability speeds up information access to boost efficiency in workflows and business planning.
- Strengthened risk management, where streamlined auditing processes reduce regulatory fines, build customer trust, cut system downtime, and lift productivity.
- Proactive regulatory compliance, enabled by strong governance structures that allow organizations to adapt swiftly to evolving policies.

Sargiotis (2024) adds that data governance delivers measurable value by:

- Driving enhanced efficiency through standardized protocols that minimize data errors, streamline workflows, and increase productivity.
- Expanding revenue opportunities by treating data as a strategic asset to uncover market trends, customer insights, and new profit avenues.
- Fueling innovation growth, as formal structures support safe experimentation with AI, analytics, and machine learning using high-quality, governed data.

Kosinski & Holdsworth (2024) notes further benefits of a well-designed data governance framework, including:

- Establishing a single source of truth (SSOT)* to ensure consistent, reliable data across the enterprise.
- Producing more accurate and trustworthy data analytics.
- Enabling safe integration of data into AI initiatives.

1.3. The Pillars of Data Governance

Data governance pillars are the fundamental elements that shape the process of data governance in organizations. Previous studies vary in the way they classify these elements, with some sources referring to them as dimensions and other sources defining them as key components of data governance. For the purpose of this study, they are synthesized and arranged in four key pillars:

1.3.1. Data Quality Management

Data quality management (DQM) is a collection of practices for enhancing and maintaining the quality of an organization's data (Gomstyn & Jonker, 2025). According to SAP (2025), "data quality refers to how relevant and reliable your data is for its intended purpose. It

* The practice of aggregating data from many systems within an organization to a single location. It is not a system or tool, but rather a state in which all data can be found via one reference point (MuleSoft, n.d.).

defines whether information can be trusted and effectively applied in daily operations or advanced data analytics" ("Data Quality Definition" section).

Data quality is often described in terms of specific dimensions, as Gupta (2020) observes, although numerous factors influence data quality, some of which are inherently context-dependent, and while no universal consensus exists on a standardized set of dimensions, the following are identified as key considerations for assessing data quality:

- **Completeness:** The extent to which data is comprehensive, reflecting the proportion of expected data collected relative to the total that exists.
- **Accuracy:** The degree to which data corresponds to reality or correctly represents the true value.
- **Consistency:** The extent to which data definitions and representations remain uniform across all observations.
- **Timeliness:** The degree to which data are both representative of current conditions and available for use.
- **Uniqueness:** The extent to which each record or entry appears without duplication.

1.3.2. Data Lifecycle Management

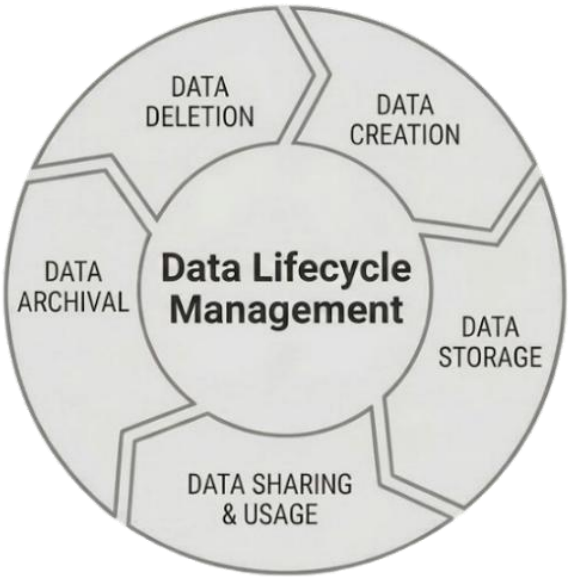
Data lifecycle management (DLM) is a comprehensive policy-based approach for managing data throughout its entire life cycle, from its creation to its eventual purging upon becoming obsolete (Eryurek et al., 2021).

International Business Machines Corporation [IBM] (2021) states that a data lifecycle consists of a series of phases through which data passes from creation to deletion. At each phase, a set of policies are applied to maximize the value derived from the data. These phases are as follows:

- **Phase 1. Data Creation:** Data is generated by a variety of sources and needs to be evaluated for quality and alignment to organizational objectives.
- **Phase 2. Data Storage:** Data is stored according to its structure, where structured data is stored in relational databases and unstructured data is stored in NoSQL databases, and should be subjected to security checks, processing, such as encryption, and backup redundancy to ensure privacy standards and ensure loss.

- **Phase 3. Data Sharing and Usage:** Data is shared with authorized users to be used in specific purposes, either internally to support analytics and decision-making or externally to support services such as marketing, and limits on usage are set by DLM.
- **Phase 4. Data Archival:** Data that is not needed in the day-to-day operations is stored as an archive in case of legal or investigative situations and DLM defines the time limits, location, duration, and recoverability.
- **Phase 5. Data Deletion:** Data that has expired its retention period or usefulness are safely removed out of all records and archives to release storage space to active data.

Figure 03: Data Lifecycle Management Phases



Source: Prepared by the author based on IBM (2021).

1.3.3. Data Stewardship and Roles

Data stewardship is the delegation of responsibility and accountability of data management and the procedures that guarantee its successful control and utilization as an organizational resource. It can be formalized by using specific job roles or it can be done informally by those individuals who work to enable the organization gain value out of its data. Practically, data stewardship usually entails metadata management and definition, data rules and standards, data quality concerns, data governance policy adherence in day-to-day operations and projects (DAMA International, 2017).

Data governance is carried out through multiple roles within an organization. The table below presents the most significant of these roles:

Table 02: Key Roles in Data Stewardship

Role	Description
Data Protection Officer	Data protection officer (DPO) is an expert in data protection who guides and oversees an organization in adherence to data protection laws, gives advice on impact analyses, and acts as a point of contact to the data protection authority and the individuals (European Data Protection Board [EDPB], n.d.).
Data Steward	Data steward has the role of ensuring that data is of quality, accurate and consistent. They collaborate with business users to get to know data requirements, create and execute data governance policies, track data quality, and fix any problems. A data steward can be in charge of several or numerous data assets, and every data domain should have at least one (Batchelder, 2024).
Data Owner	Data owner is a top-level executive who manages the strategic management of data within their scope, provides guidelines, goals, and decisions related to data, and has operational personnel reporting to him or her (Bollweg, 2022).
Data Custodian	Data custodian is in charge of technical implementation of data policies, IT infrastructure management, including databases, servers, and cloud storage, security control application, and backups, recovery, and archival operations (Bougnague, 2025).

Source: Prepared by the author based on European Data Protection Board (n.d.); Batchelder (2024); Bollweg (2022); Bougnague (2025).

1.3.4. Data Security and Compliance

Data security includes the planning, development, and execution of security policies and procedures to provide proper authentication, authorization, access, and auditing of data and information assets. The specifics of data security (which data needs to be protected, for example) differ between industries and countries. Nevertheless, the goal of data security practices is the same: To protect information assets in alignment with privacy and confidentiality regulations, contractual agreements, and business requirements (DAMA International, 2017).

A multi-layered approach that is proactive is required to ensure effective data security. According to Sargiotis (2024) There are several major measures that could enhance the safety of the data including:

- **Application of Strong Security Frameworks:** Implementation of holistic security structures such as ISO/IEC 27001 assists in establishing sound security policies and controls. This brings about an organized manner of managing data security.
- **Frequent Security Audits and Risk Assessment:** The implementation of routine security audits and risk assessments can be used to identify vulnerabilities and put things in accordance with security policies. It also enables a fast response to emerging threats.

- **Implementation of Access Controls:** Restricting data access based on users' specific roles and applying the principle of least privilege, whereby individuals are granted only the minimum permissions required for their duties, significantly reduces the risk of unauthorized access and insider threats (Plachkinova & Knapp, 2023).
- **Training and Awareness of the Employees:** The number of insider threats should be reduced by offering regular training to employees on data security practices and cyber threats. The employees are usually the first line of defense hence the need to remain informed.
- **Advanced Security Technologies:** The protection of the data is significantly enhanced using sophisticated tools such as encryption, multi-factor authentication, and intrusion detection systems. These provide high-level security against cyber threats.
- **Incident Response Planning:** An incident response plan is clear to ensure that in case of a data breach, the responses are quick and efficient. It assists in preventing the amount of damage and accelerates the recovery.

1.4. Data Governance Framework and Maturity Model

The key to organizing data governance in organizations is to understand the data governance frameworks and maturity models.

1.4.1. Data Governance Framework

A data governance framework as proposed by Sargiotis (2024) is a system of rules, policies, standards and practices that are formally described and are used to assist an organization to manage, use and protect its data resources. As a map of data management, it includes the most significant fields of data management including data quality, data security, data privacy, data lifecycle management, and compliance. The essential aspects of a data governance model are:

- **Governance Structure:** Describes the organizational design and hierarchy.
- **Decision-Making Processes:** Determine how decisions about data are made.
- **Data Policies and Standards:** Define the rules and technical specifications for data management.
- **Roles and Responsibilities:** Define the work of the individuals and groups in the governance framework.
- **Monitoring, Enforcement and Continuous Improvement:** Monitor policies, and make the framework adapt to new technology and business environment.

Figure 04: Components of a Data Governance Framework

Source: Prepared by the author based on Sargiotis (2024).

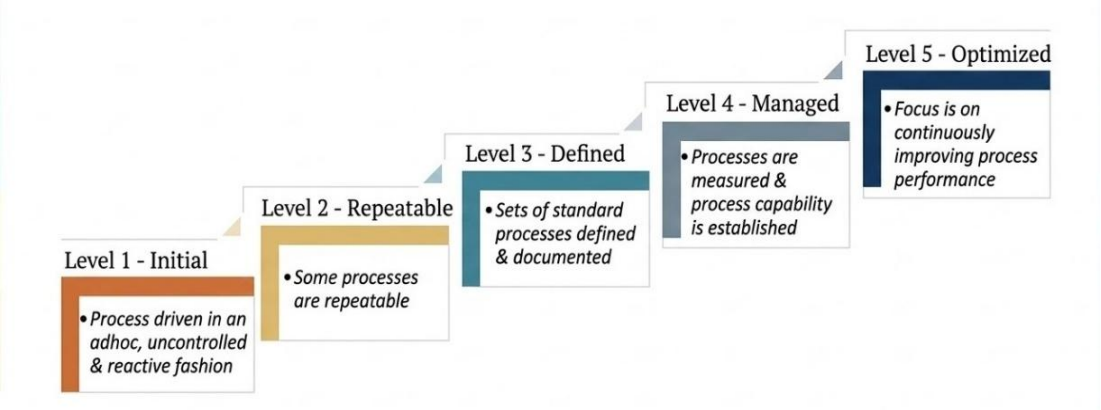
1.4.2. Data Governance Maturity Models

A maturity model is a diagnostic instrument or guiding framework that allows organizations to determine their present degree of effectiveness and competence in a particular discipline, e.g. data governance. It assists in determining the improvements and capabilities needed to achieve the desired future state and is therefore especially useful in steering the development of a data governance maturity model. Maturity models are arranged at progressive levels, which reflect growing abilities, predictability, and performance, in one or more dimensions. The higher the maturity level, the higher the capabilities and predictability and effectiveness. These levels are cumulative whereby each level is based on the base of the preceding level and it is impossible to move to the next level without mastering all the lower levels (Mahanti, 2021b).

Based on Sargiotis (2024), the stages and criteria might be different in various models, but usually, the common stages in data governance maturity models include:

- **Ad-Hoc:** No formal data governance practices, data management is decentralized.
- **Initial/Chaotic:** First attempts to build data governance, but no common processes.
- **Defined:** data governance policies are defined but not always implemented.
- **Managed:** Processes of data governance are done on a regular basis and roles and responsibilities are clearly defined.
- **Optimized:** Continuous data governance practices improvement and optimization.

Figure 05: Capability Maturity Model (CMM)



Source: Prepared by the author based on Mahanti (2021b).

Various organizations have proposed data governance maturity models. The table below shows selected models, their maturity levels, and subject areas:

Table 03: Examples of Data Governance Maturity Models

Practitioner	Maturity levels	Subject area
Kalido	4 maturity levels— • application centric • enterprise repository centric • policy centric • fully governed	3 key areas— • organization • process • technology
DataFlux	4 maturity levels— • undisciplined • reactive • proactive • governed	5 components— • people • policies • technology • risk and reward. • advancing to the next stage
Microsoft	4 maturity levels— • basic • standardized • rationalized • dynamic	3 key areas— • people • process • technology
IBM	5 maturity levels— • initial • managing • defined • quantitatively managed • optimizing	11 domains— • organizational structures and awareness • stewardship • policy • value creation • data risk management and compliance • information security and privacy • data architecture • data quality management • classification and metadata • information lifecycle management • audit information, logging and reporting

Source: Prepared by the author based on Mahanti (2021b).

2. Personal Data Protection

We live in an era in which personal data are collected, stored, and processed on an unprecedented scale. As a result, the protection of personal data has emerged as a fundamental right and a central policy challenge of the digital age, necessitating comprehensive regulation and responsible institutional conduct (Berisha et al., 2026).

2.1. Definition of Personal Data Protection

In literature, the term data protection is often used interchangeably with personal data protection. Therefore, the following definitions refer to data protection in general but are applied in this study in the context of protecting personal data:

Data Protection refers to the procedures and regulations according to which personal or official data submitted to organizations are not abused or leaked publicly (Cambridge University Press, n.d.).

Expanding on this overall idea, the term data protection is narrowed down to refer to the act of preventing the loss and corruption of sensitive information and is aimed at safeguarding data and ensuring that it is accessible and meets regulatory standards (IBM, 2024).

This process is legally established as a legal requirement that mandates organizations to make sure that their personal data is treated in a fair and lawful manner (DataGuard, n.d.).

Moreover, it is legal restrictions that make the information stored on computers confidential and determine who can access it or utilize it (Oxford University Press, n.d.).

Technically speaking, data protection is a set of security measures and procedures that prevent sensitive data from being corrupted, compromised, and lost, as well as using privacy policies to enforce compliance and safeguard the reputation of an organization against data theft, data leaks, and data breaches (Microsoft, n.d.-b).

In everyday usage, individuals often don’t distinguish between data protection and data security, often using the two terms as if they mean the same thing. While they are closely related, understanding the difference is important, Table 04 shows the distinctions between the two concepts:

Table 04: Distinctions between Data Security and Data Protection

Concept / Criteria	Data Security	Data Protection
Scope	Focuses on safeguarding data from unauthorized access, security breaches, and cyber threats.	Broader approach that includes securing data while also ensuring privacy, regulatory compliance, and ethical handling.
Primary Goal	Maintaining confidentiality, integrity, and availability of data.	Upholding privacy rights, lawful processing, and respect for individual data subjects.
Key Methods	Technical controls such as encryption, firewalls, access restrictions, and threat detection and response.	Policy-based measures including privacy policies, data minimization, consent management, and legal compliance frameworks.
Goal Considerations	Generally consistent across regions with universal security principles.	Highly variable by jurisdiction, with region-specific requirements (e.g., GDPR in Europe; HIPAA in the United States).

Source: Prepared by the author based on Vaideeswaran (2023).

2.2. Legal Framework of Personal Data Protection in Algeria

The development of digital technologies has enhanced the collection and exchange of personal data, which forced states to develop protective legislative frameworks consistent with international standards. In turn, Algeria passed the Law No. 18-07 of June 10, 2018, which is expected to both take advantage of the opportunities of the digital transformation and address the challenges of cybersecurity. The purpose of this law is to incorporate Algeria into the digital economy and act as a protective barrier against both local and international data protection issues (Imad, 2024). This framework was subsequently amended and extended by Law No. 25-11 of July 24, 2025, which introduced a Data Protection Officer requirement, mandatory processing registers, regional supervisory poles, six new legal definitions, and an entirely new title governing the processing of personal data for law enforcement purposes (Law No. 25-11, 2025).[*]

2.2.1. Overview of Laws No. 18-07 and No. 25-11

Law No. 18-07, relative to the protection of natural persons in the processing of personal data, constitutes Algeria's primary legislative instrument in this domain. As stated in Art. 1 of Law No. 18-07 (2018), its object is to fix the rules for the protection of natural persons in the processing of personal data. The law's foundational philosophy is articulated in Art. 2: all processing of personal data, regardless of origin or form, must respect human dignity,

[*] Unless otherwise indicated, all article references in this section are to Law No. 18-07 (2018). Articles prefixed '*bis.*' were inserted by Law No. 25-11 (2025).

private life, and public liberties, and must not harm the rights, honor, or reputation of individuals.

The law applies to both automated and non-automated processing of personal data contained in files, whether carried out by public or private entities established on Algerian territory or using means situated therein (Art. 4). It grants limited exemptions for personal or domestic processing, national defense and security, and certain other contexts (Art. 6, as modified by Art. 2 of Law No. 25-11, 2025; Art. 5 of Law No. 18-07, 2018). All processing operations falling within its scope are, by default, subject to a prior declaration or authorization requirement before the national authority (Art. 12).

2.2.2. Key Definitions

Art. 3 of Law No. 18-07 (2018), as extended by Art. 2 of Law No. 25-11 (2025), establishes the definitional framework underpinning the entire regulatory structure. Table 05 presents the key terms relevant to this study:

Table 05: Key Terms in Algeria's Laws No. 18-07 and No. 25-11

Term	Definition
Personal Data	Any information, regardless of its medium, concerning an identified or identifiable natural person referred to as the 'data subject' directly or indirectly, in particular by reference to an identification number or to one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity.
Data Subject	Any natural person whose personal data is the subject of processing.
Processing of Personal Data	Any operation or set of operations performed using automated or non-automated means applied to personal data, such as collection, recording, organization, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, alignment or interconnection, as well as locking, encryption, erasure, or destruction.
Consent of the Data Subject	Any freely given and informed expression of will by which the data subject or their legal representative accepts that their personal data shall be subject to manual or electronic processing.
Automated Processing	Operations carried out wholly or partly by automated means, including data recording, the application of logical and/or arithmetic operations to those data, their modification, erasure, extraction, or dissemination.
Sensitive Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership of the data subject, or data concerning their health, including genetic data.

Data Controller	Any natural or legal person, public or private, or any other entity that, alone or jointly with others, determines the purposes and means of data processing.
Processor	Any natural or legal person, public or private, or any other entity that processes personal data on behalf of the data controller.
Third Party	Any natural or legal person, public or private, or any other entity other than the data subject, the data controller, the processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
Recipient	Any natural or legal person, public authority, service, or other entity that receives communication of personal data.
Transfer or Communication	Any disclosure or communication of data brought to the knowledge of a person other than the data subject.
Service Provider	1) Any public or private entity that offers its users the possibility of communicating by means of a computer system and/or telecommunications system; 2) any other entity processing or storing computer data for such communication service or its users.
Data Closure	Rendering data inaccessible.
Biometric Data	Personal data resulting from a specific technical processing, relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm their unique identification.
Pseudonymization	The processing of personal data in such a manner that they can no longer be attributed to a data subject without recourse to additional information.
Personal Data Breach	Any security breach resulting, accidentally or unlawfully, in the destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed.
International Organization	Any entity and its affiliated bodies governed by public international law, or any other body created by or pursuant to an agreement between two or more States.

Source: Prepared by the author based on Art. 3 of Law No. 18-07 (2018) , as extended by Art. 2 of Law No. 25-11 (2025).

2.2.3. Fundamental Principles of Personal Data Protection

Title II of Law No. 18-07 (2018) establishes the fundamental principles governing personal data protection in Algeria. The following discussion does not cover all provisions of Title II, but focuses on the principles most directly relevant to the organizational operationalization of personal data protection:

The processing of personal data may only be carried out with the express consent of the data subject, who retains the right to withdraw that consent at any time. Communication of data

to third parties equally requires prior consent, unless processing is necessary for a legal obligation, the protection of the data subject's life, the performance of a contract, the exercise of a public interest mission, or the realization of a legitimate interest of the controller (Art. 7).

Art. 9 establishes a set of principles governing the lawful processing of personal data, which include:

a) processing data lawfully and fairly;
b) collecting data for specified, explicit, and legitimate purposes, and not further processing it in a manner incompatible with those purposes;
c) ensuring data is adequate, relevant, and not excessive in relation to the purposes for which it is collected or processed;
d) maintaining data that is accurate, complete, and, where necessary, up to date;
e) keeping data in a form that allows the identification of data subjects for no longer than necessary to achieve the purposes for which it was collected or processed.

2.2.4. Rights of Data Subjects

Title IV of Law No. 18-07 (2018) grants data subjects four fundamental rights that controllers are legally bound to respect and operate:

- **Right to Information:** Individuals have the right to be informed about the identity of the data controller, the purpose of the processing, and other relevant information before their personal data is collected (Art. 32).
- **Right of Access:** Individuals may obtain confirmation regarding whether their personal data is being processed and access such data (Art. 34).
- **Right of Rectification:** Individuals may request updating, rectification, erasure, or blocking of inaccurate personal data (Art. 35).
- **Right to Object:** Individuals may object to the processing of their personal data for legitimate reasons, particularly in cases related to certain uses of personal information (Art. 36).

2.2.5. Obligations of Data Controllers

Title V of Law No. 18-07 (2018), as modified and extended by Law No. 25-11 (2025), translates the law's principles into concrete organizational obligations for data controllers. The following points present the obligations most relevant to this study:

- **Confidentiality and Security of Processing:** Controllers must implement appropriate technical and organizational measures to protect personal data against destruction, loss, alteration, unauthorized access or disclosure, and any other form of unlawful processing, calibrated to the risks and nature of the data (Art. 38). Where processing is outsourced, controllers must select processors offering sufficient security guarantees, and the relationship must be formalized by a written contract specifying that the processor acts solely on the controller's instructions (Art. 39). Professional secrecy is mandatory for all people who, in the exercise of their functions, become aware of personal data, including after cessation of those functions (Art. 40). Any person acting under the authority of the controller or processor may only process personal data on the controller's instruction, except where required by legal obligation (Art. 41).
- **Data Protection Officer:** Law No. 25-11 (2025) mandates that every data controller designate a Data Protection Officer (DPO), selected on the basis of specialist knowledge of data protection law and practice, responsible for advising staff, monitoring legal compliance, and overseeing data protection impact assessments, while serving as the primary point of contact with the national authority (Arts. 41 *bis.* and 41 *bis.* 1, added by Art. 4 of Law No. 25-11, 2025).
- **Processing Registers and Operations Log:** Each controller and processor are required to maintain a register of processing activities documenting purposes, recipients, retention periods, and security measures, as well as an automated operation log recording all processing operations for the exclusive purposes of legality verification, internal control, and criminal proceedings (Arts. 41 *bis.* 2 and 41 *bis.* 3, added by Art. 5 of Law No. 25-11, 2025).
- **Logs Purpose Limitation:** The automated operation logs introduced by Law No. 25-11 (2025) are subject to strict purpose limitation. They are used exclusively for verifying the legality of processing operations, ensuring internal control, safeguarding data integrity and security, and supporting criminal proceedings, thereby reinforcing accountability and traceability within organizations (Art. 41 *bis.* 3 of Law No. 18-07, as added by Art. 5 of Law No. 25-11, 2025).
- **Breach Notification:** Furthermore, Law No. 25-11 (2025) strengthens the personal data breach notification regime by introducing a precise temporal obligation in specific contexts. In particular, the data controller must notify the national authority of a personal data breach no later than five (5) days after becoming aware of it. The notification must include the nature of the breach, its possible consequences, and the measures taken or

proposed to address it, and all breaches must be documented to enable verification of compliance (Arts. 45 *bis.* 8 and 45 *bis.* 9 of Law No. 18-07, as added by Art. 6 of Law No. 25-11, 2025)

- **Transfer of Data to a Foreign Country:** Data transfers to foreign States require prior authorization from the national authority and are conditional on the recipient State ensuring a sufficient level of protection of private life and fundamental rights. In all cases, transfers that may endanger public security or the vital interests of the State are strictly prohibited (Art. 44).

2.2.6. National Authority for the Protection of Personal Data

Law No. 18-07 (2018) establishes, under Title III, the National Authority for the Protection of Personal Data (ANPDP) as an independent administrative authority attached to the Presidency of the Republic, enjoying legal personality and financial and administrative autonomy (Art. 22). Its multi-institutional composition brings together presidential appointees, magistrates from the Supreme Court and Council of State, parliamentary representatives, a representative of the National Council for Human Rights, and representatives of seven ministries, all designated by presidential decree for a renewable five-year term on the basis of their legal and/or technical competence (Art. 23). The authority's mission is to ensure that personal data processing conforms to the law and that the use of information and communication technologies poses no threat to individuals' rights and private life, in fulfilment of which it is assigned thirteen functions ranging from issuing authorizations and receiving declarations, to imposing administrative sanctions, elaborating standards, and developing cooperation with foreign counterpart authorities (Art. 25). It maintains a national register of personal data protection to enable data subjects to exercise their rights (Art. 28) and may require secured transmission where network circulation of personal data presents a risk to individual rights and liberties (Art. 30). Law No. 25-11 (2025) further extended the authority's operational reach by establishing regional poles responsible for control and audit activities across the national territory (Art. 27 *bis*, added by Art. 3 of Law No. 25-11, 2025).

2.2.7. Sanctions and Enforcement

Law No. 18-07 (2018) establishes a graduated two-tier enforcement regime. At the administrative level (Art. 46), the ANPDP may issue warnings, formal notices to comply, provisional or definitive withdrawal of the declaration receipt or authorization, and fines. A

fine of 500,000 DA is specifically applicable to controllers refusing data subject rights or failing to make required notifications (Art. 47). The ANPDP may also withdraw authorization without delay where processing endangers national security or violates public order (Art. 48).

Criminal penalties are graduated by severity of the violation. Key thresholds include: processing without consent (Art. 55): 1–3 years' imprisonment and a fine of 100,000–300,000 DA; processing without prior declaration or authorization (Art. 56): 2–5 years and 200,000–500,000 DA; unlawful processing of sensitive data (Art. 57): 2–5 years and 200,000–500,000 DA; failure by a service provider to notify a data breach (Art. 66): 1–3 years and 100,000–300,000 DA; and unlawful cross-border transfer (Art. 67): 1–5 years and 500,000–1,000,000 DA. All penalties are doubled in cases of recidivism (Art. 74), and legal people are subject to penalties under the Penal Code (Art. 70).

2.3. Personal Data Protection Challenges

According to Zhuang (2024), the development of data protection laws faces significant implementation challenges in the digital age, including:

- Cross-border data transfer challenges, where differences in national data sovereignty rules and security risks during international transmission create legal uncertainty and expose data to potential breaches, complicating compliance for organizations operating across jurisdictions
- Technological advancements, such as AI, big data, and IoT, outpacing legislation and leaving laws unable to regulate emerging technologies effectively.
- Organizational awareness deficiencies, where entities prioritize commercial interests over security and privacy.
- Individual awareness gaps, where people share personal information online without taking necessary precautions.
- Government accountability issues, where departments collect large amounts of data without proper security management systems.

Lonzetta & Hayajneh (2018) identify compliance challenges organizations face when navigating data protection regulations, including:

- Broad and vague regulatory language, creating confusion for organizations attempting compliance.

- Technical hurdles in identifying appropriate security controls without regulatory guidance.
- Complex data flow mapping requirements to understand data storage and behavior across systems.
- Difficulty translating non-technical regulations into technical requirements, especially for small and mid-size enterprises.

Additional data protection challenges arise from the rapidly expanding data landscape, affecting both individuals and organizations, such as (Hyseni, 2024):

- Balancing security and privacy, as strong protection measures may conflict with individual control over information.
- Third-party data sharing, where organizations transfer data to vendors for analytics or marketing, often without full user awareness.
- Data visibility, requiring organizations to track what data exists, where it resides, who can access it, and how it flows.
- Identifying data requiring protection, distinguishing sensitive information like health or financial data from less critical data.
- Access control complexity, balancing diverse user roles while preventing unauthorized access to sensitive information.

Conclusion of Chapter I

This chapter has developed the theoretical and regulatory basis that the study needs to rely on before enforcing to the empirical ground. The literature, although not extensive, was disjointed, with technical, legal, and sector-specific offerings that can barely address each other, and none of which discusses about how an Algerian-based private sector company works towards complying with Laws No. 18-07 and No. 25-11. This is the gap that this research aims to address. The two fundamental constructions, namely data governance, which is the organizational framework of decision rights, roles, and controls, and the protection of personal data as a set of legally binding obligations, were explained in the conceptual framework. The relationship between them is not coincidental, governance is the mechanism through which legal requirements either become practice or remain on paper. Whether that holds true at Condor Electronics is what the chapters ahead will examine.

CHAPTER II

DATA AND METHODS

This chapter establishes the methodological foundation for empirical investigation. It begins with an organizational portrait of Condor Electronics and introduces the Information Systems (IS) Division as the specific field of study. The second section presents the research methodology, encompassing the mixed-methods design rationale, data collection instruments, and analytical tools. The chapter concludes with the sampling strategies applied to each research phase.

Section 1: Organizational Context

This section provides an overall organizational portrait of Condor Electronics. It offers an overview of the company, its historical background, its vision, mission, and values, business activities, and structural layout. It also introduces the Information Systems (IS) Division as the specific field of study in order to provide a clear understanding of the institutional framework.

1. Overview of Condor Electronics

Condor Electronics (SPA) is a private Algerian production and distribution firm that deals with consumer electronics. The company, which is based in Bordj Bou Arreridj, Algeria, was founded in 2002 and it offers a wide range of products, such as smartphones, televisions, air conditioners, refrigerators, washing machines, cookers, and more. It is this broad product line that enables the company to take on large scale projects, which dictates its involvement as one of the key players in the national industrial environment.

2. History and Background

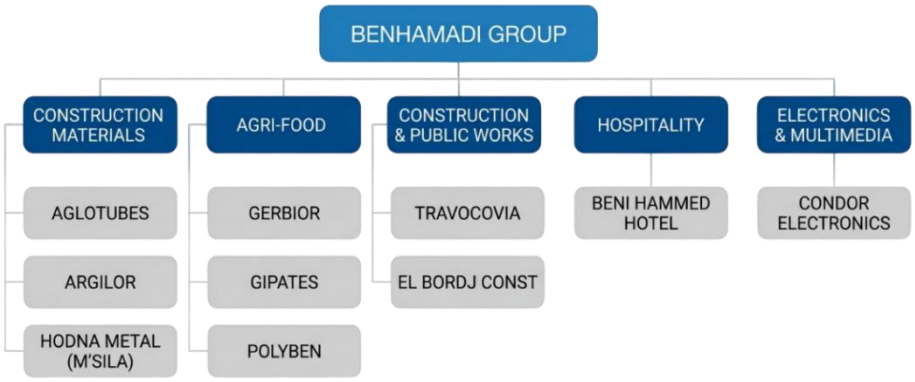
This section provides an overview of the origins and development of the parent company.

2.1. Benhamadi Group

Condor Electronics is a subsidiary of Benhamadi Group, also known as Benhamadi Group Antar Trade, an Algerian industrial conglomerate, which was established in 1948 by Mohamed Taher Benhamadi.

Over the years, the group has established considerable operational capabilities that have seen it handle a variety of business activities and projects, especially in strategic and high-impact areas. It has robust organizational and economic pillars that have helped it to maintain its status in the market. These pillars are reflected in its system of subsidiaries that help in its growth and continued expansion.

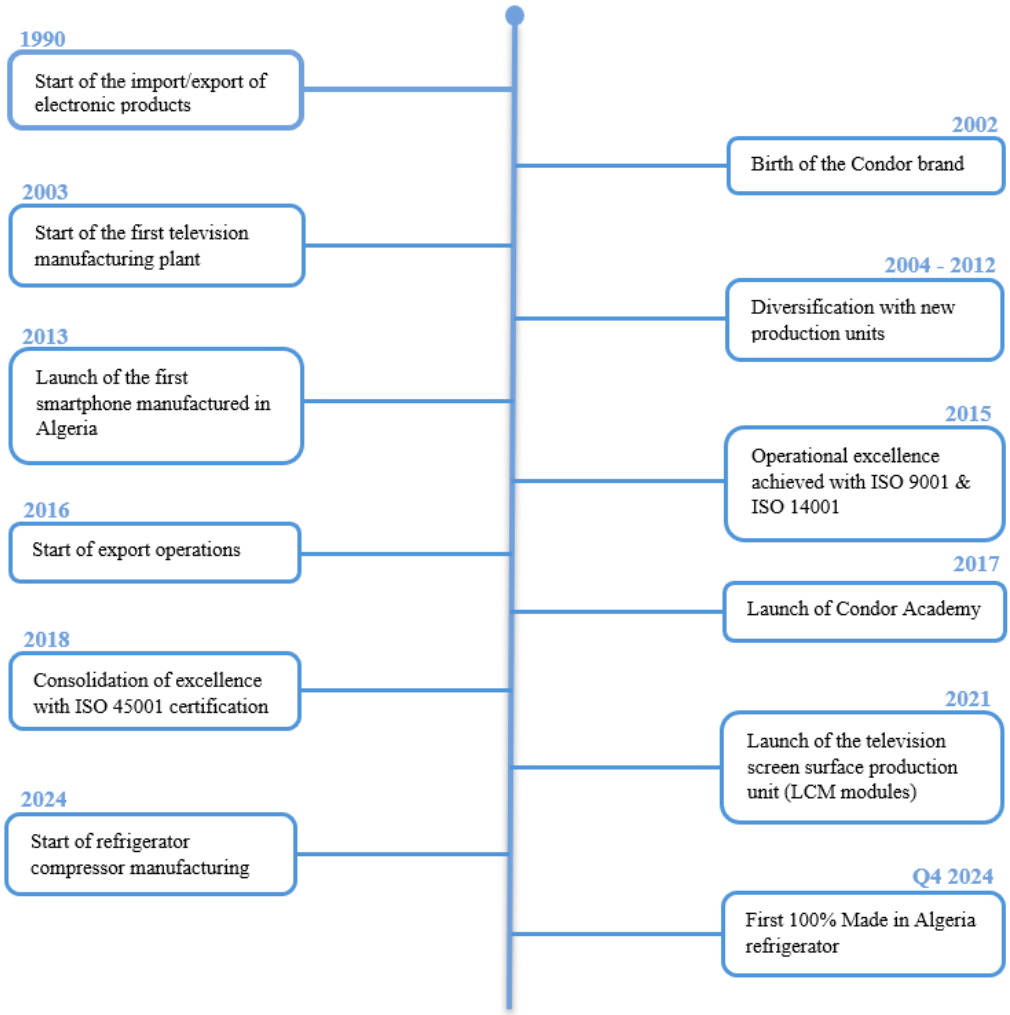
Figure 06: Organizational Structure and Business Sectors of Benhamadi Group



Source: Prepared by the author based on internal company documents.

2.2. Condor's History

Figure 07: History of Condor's Growth



Source: Prepared by the author based on Condor (2025).

3. Vision, Mission and Values

This section outlines the organization's strategic direction and core guiding principles.

3.1. Vision

Condor's vision is "To be the favorite brand in the national and regional market".

3.2. Mission

Condor's core missions are articulated as follows:

- To build a leading, sustainable and trusted group.
- Pursue controlled growth.
- Be the leader in its markets.
- Maintain employment and protect the environment.

3.3. Values

The corporate values guiding Condor are structured around six fundamental principles as illustrated below:

Figure 08: Condor's Core Values

Source: Prepared by the author based on internal company documents.

4. Business Sector

Condor operates primarily within the Electronics and Home Appliances industry, specializing in the manufacturing of a diverse range of products, from electronic devices and household appliances to IT solutions.

5. Activities

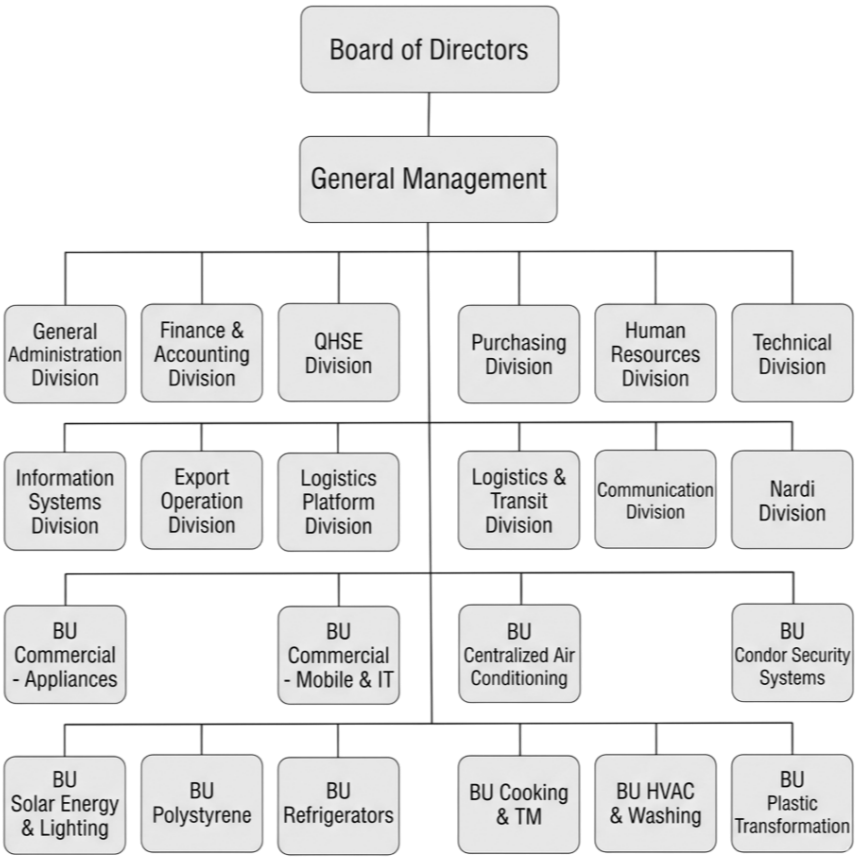
The main activities carried out by Condor Electronics encompass the following:

- **Manufacturing Activities:** It produces a wide variety of household appliances, such as air conditioners (split, cabinet, monobloc, cassette), washing machines (automatic and semi-automatic), refrigerators and freezers, cookers, gas radiators, and small home appliances.
- **Electronics Manufacturing:** Production and assembling of electronic equipment including televisions, mobile phones, tablets, satellite receivers, and electronic components including motherboards and liquid crystal modules (LCM panels).
- **Industrial Processes:** Operation of specialized production processes, including metal transformation for appliance parts and enameling lines for cookers.
- **Information Technology Services:** The supply of IT solutions to support both internal and external customers.
- **Commercial and Trade Activities:** International trading, selling own brands (Condor, Cristor, Nardi, Proxima), and partner brands (Hisense, Daikin, and SEB Group brands including Tefal and Moulinex).
- **Subcontracting Activities:** Production under license of partner brands, such as Hisense, Ace, Transsion (Infinix, Itel), Eniem, Iris, Géant, Cristo, and Nardi.
- **After-Sales Services:** Customer support services, such as maintenance, repair, call center services, and supply of spare parts, through its subsidiary.

6. Organizational Structure

Condor Electronics is organized under a Board of Directors and a General Management layer overseeing all operational and administrative functions. Six primary divisions report directly to General Management: General Administration, Finance & Accounting, QHSE, Purchasing, Human Resources, and Technical. A second tier includes the Information Systems, Export Operations, Logistics Platform, Logistics & Transit, Communication, and Nardi divisions. The organization also comprises several Business Units (BUs), notably Commercial – Appliances, Commercial – Mobile & IT, Centralized Air Conditioning, and Condor Security Systems, alongside specialized BUs such as Solar Energy & Lighting, Polystyrene, Refrigerators, Cooking & TM, HVAC & Washing, and Plastic Transformation. This structure reflects a diversified conglomerate model combining functional divisions with product-oriented business units.

Figure 09: Organizational Structure of Condor Electronics



Source: Prepared by the author based on internal company documents.

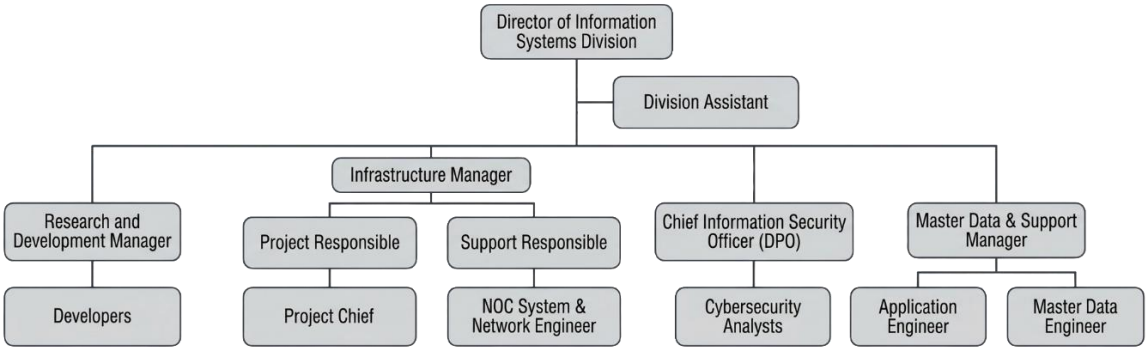
7. Field of Study (Information Systems Division)

The Information Systems (IS) Division of Condor Electronics was chosen as the main area of focus of this research because of its core functions in handling and processing the personal information of both the employees and clients of the different business units of the organization. Being the division that is directly involved in the information infrastructure that Condor operates on, it is the most relevant organizational unit in terms of which the implementation of data governance practices can be studied and how they help to protect the personal data. Moreover, the internship in this division gave first-hand experience of operational realities, key personnel and internal processes that facilitated a more grounded and contextually informed exploration of the research questions.

The IS Division serves as the backbone of a company's technological infrastructure. Essentially, this division manages the entire lifecycle of the organization’s information systems, from the initial architectural design and engineering to daily operations and maintenance. The primary responsibilities associated with these roles are outlined below:

- **Director of Information Systems Division:** Defines IS strategy and ensures alignment between information systems and organizational objectives.
- **Division Assistant:** Provides administrative and coordination support across the entire IS Division.
- **Research & Development Manager:** Leads innovation and development of new products, technologies, and technical solutions.
- **Infrastructure Manager:** Manages IT infrastructure, ensuring availability, performance, and security of systems and networks.
- **Chief Information Security Officer (DPO):** Ensures compliance with data protection regulations and oversees information security policies and risk management.
- **Master Data & Support Manager:** Governs the quality, consistency, and integrity of master data while overseeing the delivery of technical support services.

Figure 10: Organizational Structure of IS Division Main Functions



Source: Prepared by the author based on interview outcomes.

Section 2: Methodological Framework

This section outlines the research methodology adopted for the study, beginning with the mixed-methods design and the rationale for its selection. It then describes the qualitative and quantitative approaches, the corresponding data collection and analysis tools, and the sampling strategy employed.

1. Research Epistemology

This study adopts a pragmatist epistemological stance. Pragmatism, as articulated by Creswell & Creswell (2018), holds that knowledge is derived from what works in practice, and that research questions rather than a commitment to any single philosophical worldview should guide the choice of methods. Under this stance, truth and meaning emerge from the

practical consequences of inquiry, and both objective and subjective forms of knowledge are considered valid insofar as they contribute to understanding the research problem (Morgan, 2014).

The pragmatist stance was chosen because it provides the philosophical justification for combining qualitative and quantitative methods within a single study. Given that the research problem involves both measurable organizational outcomes assessed through a Likert scale questionnaire and statistical analysis, and contextual interpretive dimensions explored through observation, documentary analysis, and semi-structured interviews, no single epistemological paradigm could adequately guide the inquiry alone. Pragmatism accommodates this duality by prioritizing the research questions over methodological purity, making it the most appropriate framework for a mixed methods design of this nature (Dawadi et al., 2021).

2. Overview of Research Methodology: Mixed Methods

Mixed methods research integrates qualitative and quantitative approaches within a single study, allowing the strengths of both paradigms to be combined in order to develop a fuller and more detailed understanding of the research problem (Saraswati & Devi, 2023).

2.1. Qualitative Research

Qualitative research is a methodological approach focused on exploring the nature of phenomena by collecting and analyzing nonnumerical data such as text, video, or audio to understand feelings, ideas, and experiences. It seeks to answer questions of "why" rather than "what," aiming to gain a comprehensive understanding of social phenomena within their natural settings by examining the quality, context, and various manifestations of those phenomena (Ugwu & Eze Val, 2023).

Within this study, qualitative research was employed to explore the organizational dimensions of data governance and personal data protection that cannot be captured through numerical measurement alone. Specifically, it examines how personal data incidents and breaches are handled, the challenges faced in protecting personal data, and how governance practices overcome them. This approach goes beyond identifying the presence of practices to understanding the conditions and contextual factors shaping their implementation.

2.2. Quantitative Research

Quantitative research focuses on quantifying phenomena by collecting numerical data to answer questions such as “how many,” “how long,” or “to what degree.” It aims to generalize findings from a sample to a larger population through the systematic collection, analysis, and interpretation of quantifiable data, typically to test hypotheses (Ghanad, 2023).

For measurement purposes, quantitative research was employed to back up and validate the qualitative findings, assessing the extent to which data governance practices are implemented and their relationship with personal data protection outcomes, as well as the extent to which employees comply with personal data protection laws.

3. Reason for Choosing Mixed Methods Research

Mixed methods research is chosen because it allows the combination of the breadth of quantitative data with the depth of qualitative insights, enabling a more complete understanding of complex phenomena. This approach capitalizes on the complementary strengths of both methods, where each compensates for the limitations of the other, and facilitates triangulation to enhance validity. Additionally, findings from one method can inform the development of the other, such as using quantitative results to shape a qualitative follow-up, making the overall inquiry both rigorous and contextually rich (Dawadi et al., 2021).

4. Data Collection Methods

This section will showcase the data collection methods employed for both the qualitative and quantitative approaches within this study.

4.1. Qualitative Methods

Qualitative data collection for this study focused on observation, documentary analysis, and semi-structured interviews to examine how data governance shapes personal data protection practices.

4.1.1. Observation

Observation is a data collection method used to gather information about phenomena that can only be understood through direct viewing, including behaviors, events, and interactions in their natural settings (Ellis, 2024).

In the context of this study, observation was directed at the day-to-day data handling practices within the IS Division at Condor Electronics, including how employees interact with data systems, whether access controls are visibly enforced, how personal data is stored and transmitted, and whether governance-related procedures are visibly posted, communicated, or followed in practice. This method was employed because a low-maturity environment often presents a gap between formally stated policies and actual organizational behavior, a gap that neither survey responses nor document analysis alone can reliably capture. Direct observation allowed the gathering of contextual, first-hand evidence of governance practices as they occur naturally, without the social desirability bias that can affect self-reported responses in questionnaires or interviews

4.1.2. Documentary Analysis

Documentary analysis is a qualitative research method that involves analyzing various types of documents, including printed texts such as books, newspaper articles, academic journals, and institutional reports, as well as visual sources like photographs, video, and film. Any document containing text or visual material can serve as a source for qualitative analysis (H. Morgan, 2022).

Given that data governance and personal data protection are fields heavily grounded in formal policies, regulatory texts, and institutional standards, documentary analysis was not merely supplementary to this study but methodologically necessary. The documents examined included internal organizational documents at Condor Electronics relating to data handling policies and procedures, as well as company-held papers referencing the requirements of Algerian Law No. 18-07 and its subsequent amendments. This analysis provided an empirical basis for assessing the extent to which formal governance frameworks are reflected or absent in the organization's documented practices.

4.1.3. Semi-Structured Interviews

Semi-structured interviewing is a qualitative data collection technique that involves a verbal interaction between the interviewer and the respondent, guided by a flexible question grid. It aims to gather both factual information and insight into the respondent's experiences and perspectives, allowing the interviewer to adapt the flow of the conversation in a conversational manner (Pin, 2023).

Interview Guide: According to Roberts (2020), an interview guide is a structured yet flexible tool consisting of main questions, potential follow up probes, or an outline of key

topics. It provides organization while allowing the researcher to explore unanticipated material. The guide was used in semi-structured interviews because it balances consistency and flexibility. As Roberts explains, it keeps the interviewer and participant focused, ensures key areas are covered, supports novice researchers, and allows spontaneous follow up questions and exploration of unexpected themes, all central to semi structured interviewing.

The interviews were conducted with purposively selected participants whose professional roles and responsibilities were directly relevant to the study's research questions, ensuring that the data collected would yield substantive and operationally grounded insights into data governance and personal data protection practices at Condor Electronics. During each interview, the guide was employed as a structural reference rather than a rigid script; while it ensured that all key thematic areas were systematically addressed, an open and conversational dynamic was maintained that encouraged participants to elaborate freely and introduce dimensions beyond those explicitly anticipated. This balance between structure and openness proved particularly valuable in capturing nuanced experiential knowledge that would not have emerged through a purely standardized instrument. Rather than verbatim transcription, active notetaking and keyword recording were relied upon throughout each session, a technique that allowed for the real-time identification and documentation of the most pertinent and analytically relevant elements of each response without disrupting the natural flow of the conversation. For the interview guide used during data collection, refer to Appendix A.

Choice of Questions: The semi-structured interview questions were selected in direct alignment with the conceptual framework underpinning this study, which operationalizes data governance across four measurable dimensions: data quality management, access control and data security, data lifecycle management, data policies and assigned roles. Each question targets one or more of these dimensions without using specialist terminology, so that respondents unfamiliar with formal data governance concepts could engage meaningfully with the questions based on their lived operational experience. This deliberate simplification was employed as a methodological precaution in anticipation of an environment where data governance maturity may be low and specialized terminology is not in common circulation, thereby ensuring that participants are not alienated by abstract governance language but are instead guided to describe concrete day-to-day practices. Questions were further designed to elicit responses relevant to the dependent variable ‘personal data protection’ by exploring awareness, incident handling, compliance behavior,

and role of data governance, thereby enabling qualitative triangulation with the quantitative findings of the survey instrument.

4.2. Quantitative Method (Questionnaire)

A research questionnaire is a data collection tool consisting of a series of questions or items used to gather information from respondents about their knowledge, opinions, attitudes, beliefs, and behavior. It can be understood either as a standardized instrument for producing knowledge in line with a positivist philosophy or as an encounter between researcher and respondent where knowledge is negotiated through a distinct form of communication (Ranganathan & Caduff, 2023).

The questionnaire was administered to employees of the IS Division at Condor Electronics, which constitutes the study's target population. Distribution combined digital and direct in-person channels to ensure comprehensive reach across the division. The questionnaire was made accessible via Google Forms, with a QR code generated for this purpose; in addition to being shared through the company's official internal email system and Microsoft Teams group channels dedicated to IS division staff, the QR code was presented directly to employees through individual in-person visits conducted across all available workstations within the division. This combined approach was adopted to maximize response rates while accommodating employees' varying work rhythms and schedules.

Design of the Questionnaire: The questionnaire was structured into six thematic sections, each corresponding to a specific dimension of the study's conceptual framework. The first section collected socio-demographic data (gender, age, educational level, and years of experience). Sections two through five measured the four sub-dimensions of the independent variable (Data Quality Management, Security and Access Control, Data Lifecycle Management, and Governance Policies and Roles) each composed of four Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree), for a total of sixteen questions in these sections. The sixth and final section, comprising fourteen questions, measured the dependent variable of Personal Data Protection, covering aspects such as accuracy and integrity of personal data, confidentiality, data minimization, retention practices, individual rights awareness, and employee competence. This structure was designed to test the study's main hypothesis (that data governance practices positively influence personal data protection) as well as to answer the two sub-questions: to what extent data governance practices are implemented in Condor, and to what extent Condor employees comply with personal data

protection regulations. Each set of items was crafted to capture employees' direct operational experience rather than abstract perceptions, enabling the hypotheses to be tested empirically through simple linear regression, multiple linear regression, and Pearson correlation analysis. For the questionnaire questions, refer to Appendix B.

5. Data Analysis Methods

In this section, the analytical techniques employed to process and interpret the collected data are described. The goal is to explain how raw data were transformed into meaningful insights that address the research questions and hypotheses.

5.1. Qualitative Analysis

Qualitative analysis was conducted using thematic and content analysis alongside NVivo software. The data were systematically coded, organized, and examined to identify key themes and patterns, allowing for a clear and structured interpretation of the findings.

5.1.1. Thematic Analysis

Thematic analysis is a research method used to identify and interpret patterns or themes within a dataset, often leading to new insights and understanding. It involves a systematic process of coding data, grouping codes into meaningful themes, and interpreting those themes to develop conceptual models grounded in the data (Naeem et al., 2023).

Thematic analysis was applied as the primary interpretive method for the qualitative data collected through observation and interviews. It was used to analyze both direct observations of practices within the IS Division and the accounts provided by key informants. By systematically coding recurring patterns across these two sources, this method enabled a deeper interpretation beyond surface description, constructing a coherent account of how data governance shapes, or fails to shape, personal data protection in the organization's daily functioning.

5.1.2. Content Analysis

Content analysis is a systematic, rule-guided method for analyzing text that emphasizes understanding the material within its communication context. It uses an empirical, methodologically controlled approach, follows step-by-step analytical models, and avoids premature quantification. The goal is to make specific, replicable, and valid inferences from the text to other aspects or properties of its source (such as the communicator's experiences,

opinions, or the socio-cultural background). It examines not only the manifest (explicit) content but also latent content, including themes, main ideas, and contextual information (Mayring, 2000).

In this study, content analysis was applied to the policy documents collected at Condor Electronics in order to systematically examine their content in relation to data governance and personal data protection practices. The analysis focused on both the explicit content of the policies and their latent content, including the governance logic underlying each provision and its implications for personal data protection, with the objective of producing a structured mapping between documented organizational practice and the theoretical dimensions under investigation.

5.1.3. NVivo

NVivo is a computer-assisted qualitative data analysis software (CAQDAS) program that helps researchers collect, organize, visualize, and report qualitative data. It can import and support multiple data formats and is a useful tool for sorting and managing multifaceted qualitative information (Dhakal, 2022).

NVivo 15 was selected as the analytical platform for the qualitative phase of this study due to its capacity to handle and systematically organize unstructured textual data derived from semi-structured interviews. The four transcripts were subjected to four complementary analytical approaches: lexical analysis to examine terminology patterns, linguistic analysis to interpret discourse structure, cognitive mapping to represent the conceptual relationships and associations between themes raised by participants, and thematic analysis to identify recurring themes across participants. NVivo addressed the complexity of applying these layers simultaneously by enabling the structured importation of transcripts and the application of a systematic coding framework, through which recurring themes, sub-themes, and representative extracts were identified, labelled, and organized into nodes. The software was used to map coded segments onto the study's core dimensions of data governance and personal data protection, facilitating cross-participant comparison to identify areas of convergence and divergence in the qualitative findings.

5.2. Quantitative Analysis (SPSS)

IBM SPSS (Statistical Package for the Social Sciences) is defined as “a comprehensive statistical analysis platform designed to help organizations and individuals extract reliable insights from data. It combines robust statistical testing, predictive modeling, regression and

forecasting with streamlined data preparation and automated analysis to empower users to move confidently from data to defensible, data-driven decisions" (IBM, n.d., "Overview" section).

SPSS Statistics 31 was selected as the statistical analysis platform for the quantitative phase of this study owing to its comprehensive suite of tools for descriptive and inferential analysis and its widespread validation in academic survey-based research. The software was used to compute Cronbach's alpha coefficients to assess internal consistency reliability, generate descriptive statistics for all scale items, perform simple linear regression to test the predictive relationship between the independent and dependent variables, calculate Pearson correlation coefficients to examine the relationships between data governance sub-dimensions and personal data protection, enabling the empirical testing of the study's main hypothesis and sub-hypotheses.

6. Research Sample

A research sample refers to a subset of individuals or elements selected from a larger population for the purpose of analysis and data collection. Instead of studying the entire population, researchers rely on sampling to obtain reliable and representative information in a more efficient and practical way. This approach is particularly useful when the population is large, as it reduces the time, cost, and effort required while still allowing for accurate conclusions about the whole population (Makwana et al., 2023).

In the present study, sampling was applied across both the quantitative and qualitative strands of the mixed-methods research design, each governed by its own logic and selection criteria suited to the nature of the data being sought. The following sections detail the sampling strategy, size, and rationale specific to each phase.

6.1. Qualitative Sample

The qualitative sample for the semi-structured interviews consisted of four participants; each selected on the basis of their professional function and its direct relevance to the study's research questions. All participants are employed within or in close institutional relation to the IS Division at Condor Electronics, and together they represent a cross-section of the organizational roles most implicated in data governance and personal data protection practices. As shown in Table 06, the sample spans technical, legal, security, and human resources functions, with cumulative professional experience ranging from 3 to 11 years and

interview durations ranging from approximately 45 to 90 minutes. This diversity of professional perspectives was intentional, as it enables a more comprehensive and multi-dimensional understanding of how data governance is implemented and experienced across different organizational roles.

Table 06: List of Interviewees

No.	Name	Function	Experience	Duration
1	M. E.	Chief Information Security Officer	11 years	≈ 45 min
2	B. N.	Human Resources Officer	10 years	≈ 90 min
3	O. S.	Information Systems Engineer	8 years	≈ 60 min
4	G. Z.	Legal Affairs Officer	3 years	≈ 45 min

Source: Prepared by the author.

6.2. Quantitative Sample

The target population of this study consists of the employees of the IS Division at Condor Electronics, estimated at 80 available employees at the time of data collection. Given that this population is finite and relatively small, the formula developed by Krejcie & Morgan (1970) was selected to determine a statistically justified minimum sample size. This formula was chosen for its suitability in studies involving finite populations and its widespread validation in social science research. The formula is expressed as follows:

$$s = \frac{X^2 NP(1-P)}{d^2(N-1) + X^2 P(1-P)}$$

Where:

- s = required sample size
- X^2 = chi-square value for 1 degree of freedom at the 95% confidence level (3.841)
- N = population size (80)
- P = population proportion (0.50, maximizing sample size)
- d = margin of error (0.05)

Substituting the values:

$$s = \frac{3.841 \times 80 \times 0.5 \times (1 - 0.5)}{(0.05)^2 \times (80 - 1) + 3.841 \times 0.5 \times (1 - 0.5)}$$

$$s = \frac{76.82}{0.1975 + 0.96025}$$

$$s = \frac{76.82}{1.15775}$$

$$s \approx 66$$

The formula yields a minimum required sample of 66 respondents, a result consistent with the reference table provided by Krejcie & Morgan (1970). Through the distribution channels described in the preceding section, 67 complete and valid responses were collected, exceeding the statistically determined threshold and fully satisfying the sampling requirement. The sample is therefore considered adequate for the inferential analyses conducted in this study, including Pearson correlation and simple linear regression.

Conclusion of Chapter II

This chapter has provided the institutional setting and laid out the methodological architecture through which the research questions and hypotheses of this study are to be empirically addressed. The organizational portrait of Condor Electronics and its Information Systems (IS) Division established the contextual grounding necessary for interpreting the findings that follow. The mixed-methods design was shown to be the most appropriate approach for a study of this nature, as it enables the quantitative measurement of data governance practices and their relationship to personal data protection outcomes to be complemented by the qualitative depth needed to understand how those practices are experienced, implemented, and constrained within the organizational reality of Condor Electronics. The data collection instruments, the questionnaire distributed to all available employees within the IS Division, which yielded 67 complete and valid responses, and the semi-structured interviews conducted with four purposively selected participants, were each designed in direct alignment with the study's conceptual framework. The analytical methods and sampling strategies have been justified and calibrated to the specificities of the research environment. The empirical findings generated through this framework are presented and interpreted in the chapter that follows.

CHAPTER III

RESULTS AND DISCUSSION

This chapter presents and interprets the empirical findings generated through the mixed-methods approach adopted in this study. The first section is devoted to the presentation and analysis of results, organized into two strands: the qualitative findings drawn from field observation, documentary analysis, and semi-structured interviews, followed by the quantitative findings derived from the administered questionnaire. The second section discusses these findings in depth, addressing the study's research questions and hypotheses through triangulation across all data sources, situating the results within the existing literature, and drawing analytical conclusions about the role of data governance in personal data protection at Condor Electronics.

Section 1: Results Presentation and Analysis

This section presents and analyzes the empirical results obtained through the mixed-methods approach adopted for this study. Qualitative findings are examined first, encompassing field observation, documentary analysis, and semi-structured interviews, before turning to the quantitative findings derived from the administered questionnaire.

1. Qualitative Results

The qualitative strand of this study draws on three complementary sources: field observation conducted within the Information Systems Division, documentary analysis of nine policy documents, and semi-structured interviews with key informants. The findings from each source are presented in turn below.

1.1. Observation

Direct observation of the IS Division at Condor Electronics yielded three principal themes relating to data governance and personal data protection practices.

- **Theme 1: Operational Data Governance Practices**

Observation of the IS Division revealed the existence of governance policies, including data-related policies, visibly present within the departmental environment in both digital and physical form. These policies represent the primary evidence of data governance practice identified through direct observation. Their content and scope will be examined in detail in the documentary analysis sub-section that follows. Additionally, the GLPI platform was observed to be in active use as a formalized internal tool through which employees both submit access requests to obtain data from designated data owners and report operational issues; an example of such reported issues is the correction of erroneous or inconsistent data

values when identified. This use of GLPI constitutes an observable mechanism through which data stewardship activities and access control management are executed within the organization.

- **Theme 2: Data Protection Awareness and Legal Compliance**

Two convergent indicators of data protection awareness were directly observed. Data awareness sessions conducted for new employees were attended on multiple occasions, during which staff were informed of the security procedures and measures required to safeguard organizational data and comply with the provisions of Algerian Law No. 18-07. Additionally, the division's data security policy was found to be physically displayed throughout the workspace, explicitly referencing the protection, integrity, and proper management of information in accordance with legal and security requirements. Two categories of compliance documentation were also examined: agreement documents submitted to the ANPDP pertaining to the transfer of personal data to foreign cloud servers, and declaration documents specifying the retention periods applied to different categories of personal data, further details of which are provided in Appendix C. Together, these observations indicate the presence of data protection awareness practices and documented engagement with the national supervisory authority across key compliance obligations.

- **Theme 3: Absence of a Formal Data Governance Framework**

Operational practices are present, but no formal data governance framework exists. Roles resembling data owners, custodians, and a data protection officer are performed informally and identified by job titles rather than clearly defined governance responsibilities, while the data steward role is absent. Although an IS Standards and Governance Manager position, which represents the closest approximation to a formal governance function, appears in organizational documentation, interview data confirmed that it has remained vacant since 2023 and was subsequently removed without replacement. The vacancy of this position since 2023 and its subsequent removal without replacement represent a structural absence in the organization's governance architecture, the implications of which will be examined through triangulation with the remaining data sources.

1.2. Documentary Analysis

The following sub-section presents the findings of the documentary analysis conducted on the policy documents collected at Condor Electronics. All policies examined were updated in 2025 in accordance with ISO 27001:2022. Each policy follows a standardized structure comprising at minimum eight common sections:

(1) **Purpose**, which defines the objective and rationale of the policy;
(2) **Scope**, which delimits the systems, data, and personnel to which the policy applies;
(3) **References**, which lists the regulatory, normative documents underpinning the policy;
(4) **Definitions and Abbreviations**, which clarifies the key terms and acronyms used throughout the document;
(5) **Responsibilities**, which assigns accountability for implementation and compliance to specific roles and divisions;
(6) **Description of the Policy**, which constitutes the core body of the document detailing the rules, procedures, and controls to be applied;
(7) **Review**, whereby all policies are subject to mandatory annual review to account for any organizational, technical, or legislative changes; and
(8) **Disciplinary Measures**, stipulating that non-compliance will result in disciplinary measures in accordance with Condor Electronics' internal regulations.

It should be noted that individual policies may contain additional sections beyond this common structure depending on their specific scope and requirements. An example of a policy document is provided in Appendix C.

A qualitative content analysis approach was adopted for the examination of the policy documents collected at Condor Electronics, following Mayring's (2000) framework. The analysis was predominantly deductive, with coding categories derived from the study's theoretical framework on data governance. One category (Information Classification and Data Categorization) emerged inductively from the documents themselves, as no equivalent dimension was identified in the pre-established framework. Each policy provision was systematically assigned to the category it most directly addresses. The following table presents the coding scheme applied:

Table 07: Content Analysis Coding Scheme

Category	Policy Document	Pages	Key Provision
Information Classification and Data Categorization	**Information Systems Asset Management Policy**	p.7-8	Four-tier data classification schema (Public, Internal, Confidential, Restricted)
	Cloud Migration Strategy Policy	p.9-10	Three-type data typology (sensitive personal, strategic, business application)
Access Control and Security	**Information Systems Access Control Policy**	p.4-5	Governance hierarchy: DSI, IT Infrastructure Manager, IT Security Manager, HR, BPO
		p.7-9	Formal user registration/de-registration; need-to-know provisioning; quarterly access review; immediate deactivation on termination
		p.10-12	Password complexity; 2FA; session timeout; lockout policy; restricted system utilities; mandatory version control
	Cloud Services Security Policy	p.7	Least Privilege Principle; MFA; PAM; continuous access logging
Data Lifecycle Management	**Operations Security Policy**	p.8	Backup procedures; RPO/RTO definition; quarterly backup testing; minimum 1-year log retention; geographically distributed storage
	Cloud Services Security Policy	p.4, 9	Secure erasure upon service termination; verified by audits or destruction certificates
		p.8	Regular backups; secure storage; periodic integrity checks
	HR IS Security Policy	p.7	Access privilege modification before role change; formal return of all information assets on termination
Legal and Regulatory Compliance	**Cloud Migration Strategy Policy**	p.10	Explicit requirement to update the data protection governance model; define stakeholder roles and responsibilities matrix; involve legal department; rigorous monitoring of compliance with legislative framework
	Compliance Policy	p.5-6	Regulatory monitoring program; internal compliance program directed by CISO; periodic review; external audits
	Security Incident Management Policy	p.4, 10	Structured incident response cycle; personal data breach defined with reference to Law No. 18-07

	Cloud Services Security Policy	p.6, 8	ANPDP authorization required for cross-border data hosting; provider evaluation based on hosting country regulations
		p.10	Regulatory non-compliance identified as explicit risk category regarding Algerian law
	Communications Security Policy	p.7-8	Information transfer controls; NDA mandatory for all employees, suppliers, and subcontractors; annual legal review
	HR IS Security Policy	p.6	Annual security awareness training for all staff; KPI-monitored effectiveness; records kept for audit

Source: Prepared by the author.

- **Category 1: Information Classification and Data Categorization**

A structured approach to information classification was identified across two policy documents. The Information Systems Asset Management Policy establishes a four-tier classification schema (Public, Internal, Confidential, and Restricted) applicable to all information assets, with the latter two categories governed on a need-to-know basis and classification performed by the asset owner based on legal, contractual, and sensitivity criteria (Information Systems Asset Management Policy, p.7-8). The Cloud Migration Strategy Policy complements this with a cloud-specific data typology distinguishing between sensitive personal data, strategic company data, and business application data as a prerequisite for adequate protection prior to migration (Cloud Migration Strategy Policy, p.9-10). While these frameworks provide the foundational basis for differentiated data protection, their distribution across separate context-specific policies rather than a single consolidated governance document suggests a fragmentation that may affect consistent application across the organization.

- **Category 2: Access Control and Security**

Access control is the most elaborately documented governance practice across the policy corpus. The Information Systems Access Control Policy establishes a formal governance hierarchy, with the director of IS holding approval authority, the IT Infrastructure and Security Managers responsible for technical enforcement, HR responsible for communicating employee status changes, and Business Process Owners defining application-level access rights, and mandates need-to-know provisioning with prior

authorization required before any access is granted (Information Systems Access Control Policy, p.4-5). User accounts follow a standardized naming convention to ensure traceability, access rights are reviewed quarterly, privileged accounts must remain separate from standard accounts, and accounts must be immediately deactivated upon termination (Information Systems Access Control Policy, p.7-9). Technical controls include password complexity requirements, two-factor authentication for critical systems, session locking after ten minutes of inactivity, lockout after five failed attempts, restricted use of system utilities, and mandatory version control for source code access (Information Systems Access Control Policy, p.10-12). At the cloud level, the principle of least privilege, multi-factor authentication, privileged access management, and continuous access logging are additionally mandated (Cloud Services Security Policy, p.7). The convergence of hierarchical accountability, operational procedures, and layered technical controls across multiple policies positions access governance as the most institutionally mature practice identified in the documentary analysis.

- **Category 3: Data Lifecycle Management**

Data lifecycle governance was evidenced across three policy documents. The Operations Security Policy mandates backup procedures with defined RPO and RTO for each system, quarterly backup testing, geographically distributed storage in fireproof controlled-access facilities, formalized restoration requests directed through the CISO, and a minimum one-year retention period for restoration logs, with all retention periods explicitly required to account for legal, contractual, and regulatory obligations (Operations Security Policy, p.8). The Cloud Services Security Policy requires secure erasure upon service termination verified by audits or destruction certificates, regular cloud backups with periodic integrity checks (Cloud Services Security Policy, p.4, 8, 9), and the HR IS Security Policy mandates access privilege modification before any role change and formal return of all information assets upon termination of employment (HR IS Security Policy, p.7). While these provisions establish a structured approach to data continuity and disposal, their scope remains primarily technical and infrastructure-oriented, with non-infrastructure data categories such as HR records and customer personal data not addressed in equivalent depth.

- **Category 4: Legal and Regulatory Compliance**

Regulatory compliance with personal data protection legislation is the most cross-cutting theme across the corpus. The Cloud Migration Strategy Policy is the only document to

explicitly use the term "data protection governance model", requiring its update as part of any cloud migration through a stakeholder roles matrix, involvement of all departments including legal, and rigorous monitoring aligned with the legislative framework (Cloud Migration Strategy Policy, p.10). The same policy identifies regulatory non-compliance regarding cross-border data transfers as an explicit risk category, alongside broader data security risks including loss of control over data processing, technological dependency on the cloud provider, and breaches affecting availability, confidentiality, and integrity during migration (Cloud Migration Strategy Policy, p.10). The Compliance Policy establishes a regulatory monitoring program jointly managed by the security officer and legal department, with an internal compliance program directed by the CISO incorporating vulnerability scanning, configuration reviews, source code reviews, and incident investigations, complemented by periodic independent external audits (Compliance Policy, p.5-6). The Security Incident Management Policy classifies the unauthorized disclosure of customer personal data (defined in alignment with Law No. 18-07) as a formal incident category subject to a structured response cycle covering reporting, containment, eradication, recovery, and post-incident capitalization (Security Incident Management Policy, p.4, 10). The Cloud Services Security Policy requires ANPDP authorization before hosting data abroad and evaluates providers on their hosting country's regulations and security certifications (Cloud Services Security Policy, p.6, 8). The Communications Security Policy mandates information transfer controls and NDA obligations for all employees, suppliers, and subcontractors, reviewed annually by the legal team (Communications Security Policy, p.7-8), and the HR IS Security Policy establishes a KPI-monitored annual security awareness program formally recorded for audit purposes (HR IS Security Policy, p.6).

- **Overall Analysis**

The nine policy documents identified as most relevant to this study reflect how data governance and personal data protection are institutionalized within Condor Electronics. Read as a whole, they reveal both strengths and limits. Classification frameworks formally recognize personal data as a distinct and sensitive category, providing the basis for differentiated protection. The access control framework, the most elaborately developed across the corpus, serves as the primary operational instrument for preventing unauthorized access. Lifecycle provisions address data continuity and secure disposal, while legal and regulatory compliance provisions, anchored in Law No. 18-07, transform these practices into enforceable obligations reinforced by the ANPDP requirement, the incident response

framework, and contractual confidentiality obligations. Critically, however, these provisions are not consolidated within a single overarching framework but are fragmented across functionally separate documents without a unifying structure to coordinate them. Compounding this, no provisions governing the accuracy, completeness, consistency, or integrity of personal data were identified across the entire corpus, a significant gap given that data quality is a foundational dimension of mature data governance. Together, these structural absences suggest that governance efforts have been directed primarily toward securing access to data rather than managing it comprehensively, a pattern consistent with the low maturity profile identified through observation and one that will be further explored through the remaining data sources.

1.3. Interviews

To draw fully on the richness of the qualitative corpus collected, the interview data was analyzed using a multidimensional textual analysis approach, structured around four complementary analytical layers, all conducted through NVivo 15:

- The lexical approach, which identifies the most frequently recurring terms across the four transcripts, revealing dominant concepts and thematic preoccupations;
- The linguistic approach, which examines forms of expression, verb usage, and rhetorical structures reflective of participants' attitudes and perceptions;
- Cognitive mapping, which aims to represent the conceptual relationships and associations between themes raised by participants;
- The thematic analysis, which organizes participants' responses according to the study's core analytical dimensions in order to address the research questions.

1.3.1. Lexical Approach

A word frequency query was conducted on the interview transcripts using NVivo, with a custom stop list applied to filter out common functional words and retain only semantically meaningful terms. The analysis was restricted to the 25 most frequent words, as these best capture the dominant themes emerging from the data. The results are presented in Table 08 below.

Table 08: Top 25 Most Frequent Words in Interview Transcripts

Rank	Word	Count	Weighted %
1	data	147	6.50%
2	personal	39	1.72%
3	access	31	1.37%
4	employee	25	1.10%
5	protection	24	1.06%
6	department	23	1.02%
7	formal	21	0.93%
8	legal	21	0.93%
9	organization	19	0.84%
10	compliance	18	0.80%
11	policies	17	0.75%
12	management	16	0.71%
13	security	16	0.71%
14	incident	13	0.57%
15	quality	13	0.57%
16	information	12	0.53%
17	system	12	0.53%
18	ciso	11	0.49%
19	request	11	0.49%
20	control	10	0.44%
21	human	10	0.44%
22	officer	10	0.44%
23	team	10	0.44%
24	awareness	9	0.40%
25	deletion	9	0.40%

Source: Prepared by the author using NVivo 15.

"Data" dominates with 147 occurrences, unsurprisingly given the subject matter. More significant is "personal" (39 occurrences), which appeared consistently as part of the compound "personal data" across all four roles and all question topics, confirming that responses were framed within a personal data protection register rather than a generic technical one. "Access" (31 occurrences) and "control" (10 occurrences) appeared almost exclusively in procedural clusters: the multi-step access request workflow and the least-privilege principle, confirming that access control at Condor is operationalized rather than merely stated as policy. "Request" (11 occurrences) reinforces this, appearing exclusively in the context of formal access demand submissions through the GLPI platform.

"Employee" (25 occurrences) carried a dual meaning: in lifecycle and stewardship responses it referred to the individual whose data is handled, while in Q8 responses all four participants used it to describe the primary source of non-compliance, namely resistance to change and informal communication habits. "Human" (10 occurrences) consistently appeared alongside this risk framing, used exclusively in the context of human error as a governance vulnerability. "Awareness" (9 occurrences) appeared either in policy dissemination mechanisms or as a named vulnerability, with three of four participants identifying insufficient awareness as the primary human-factor risk.

"Formal" (21 occurrences) marked three distinct uses: documented procedures, structured training, and contrast with informal behavior. The DPO used it in direct opposition to employees bypassing sanctioned channels via WhatsApp, meaning the term describes a gap as much as an achievement. "Compliance" (18), "policies" (17), and "legal" (21) were grounded in specific referents such as KPI monitoring, audits, disciplinary consequences, and the provisions of Laws 18-07 and 25-11, with variation in self-reported implementation rates across participants reflecting real departmental differences.

"Protection" (24 occurrences) appeared almost exclusively alongside "personal data," functioning less as a standalone concept and more as the normative objective that all other governance activities were described as serving. "Security" (16 occurrences) was used in two distinct contexts: technical security measures such as firewalls and surveillance systems, and the broader organizational security posture governed by the CISO and his "team" (10 occurrences), the latter term appearing consistently as a collective attribution of responsibility rather than individual ownership. "Management" (16 occurrences) spanned multiple governance dimensions, appearing in the context of access management, data

lifecycle management, and the management of incidents and quality issues. "Quality" (13 occurrences) appeared exclusively in departmental descriptions of data accuracy practices and audit-based quality assurance mechanisms.

"Department" (23 occurrences) and "organization" (19 occurrences) reflect the institutional framing dominant across all transcripts, with participants consistently situating governance practices within departmental or organizational structures rather than individual responsibilities. "Officer" (10 occurrences) and "ciso" (11 occurrences) reflect the concentration of formal data protection responsibility within specific designated roles, with the CISO emerging as the central governance actor referenced across all four interviews. "Information" (12 occurrences) and "system" (12 occurrences) appeared primarily in references to the Information Systems Division and the technical systems through which data is managed, stored, and protected.

"Incident" (13 occurrences) appeared either in descriptions of the formal response plan or in the uniform statement, repeated by three of four participants, that no breach has occurred to date, meaning the framework exists but has not been tested in practice. "Deletion" (9 occurrences) surfaced the sharpest governance tension in the corpus, with the Legal Department explicitly withholding deletion pending potential judicial obligations while the DPO described a formalized destruction procedure including physical media destruction and documented records, constituting direct evidence of uneven lifecycle governance within the same organization.

Figure 11: Word Cloud of Most Frequent Terms in Interview Transcripts

Source: Prepared by the author using NVivo 15.

The word cloud confirms the patterns identified in Table 08. The visual dominance of "personal," "data," "access," "employee," and "formal" corresponds directly to their high frequency counts. The spatial distribution of terms also illustrates the breadth of topics covered across interviews, spanning governance structures, legal obligations, security measures, and human factors, all of which align with the study's research questions and the four dimension pairings of the conceptual framework.

Figure 12: Items Clustered by Word Similarity

Source: Prepared by the author using NVivo 15.

The cluster analysis groups the four participants by lexical similarity across their transcripts. The HR Officer, Data Protection Officer, and IS Engineer form a tight cluster, with Pearson correlation coefficients ranging from 0.83 to 0.90, reflecting their shared operational vocabulary around access control, data lifecycle, and security procedures. The Legal Affairs Officer sits apart, recording lower similarity scores with all three participants (0.72 to 0.76), which is consistent with the interview content: their responses were distinctly shaped by litigation-oriented concerns, judicial retention obligations, and a departmental scope that differs structurally from the IS-facing roles. This separation is not indicative of disagreement on governance principles but of role-specific language, and it reinforces the value of having sampled across departments rather than within a single function. Refer to Appendix D for full Pearson correlation coefficients.

Taken together, the lexical analysis provides an initial mapping of the thematic landscape of the corpus. Word frequency confirms that the key constructs of the study are substantively present in the data, while the cluster analysis reveals that participants engaged with them from distinct role-based perspectives. The following sections build on this foundation, moving toward the thematic analysis where responses are examined in depth against the study's core analytical dimensions.

1.3.2. Linguistic Approach

The linguistic approach examines the forms of expression used by participants across the four interview transcripts, focusing on verb usage, language register, and the way ideas are formulated.

A dominant feature across all transcripts is the use of passive and impersonal constructions such as "data is retained," "corrections are applied," and "the incident is then reported." This institutional register is consistent across all four participants regardless of their role, reflecting a discourse rooted in procedure and organizational obligation rather than personal initiative. Action verbs appear frequently in procedural descriptions: "control," "ensure," "prevent," "verify," "submit," and "notify" recur across responses, signaling a compliance-oriented framing in which data governance is understood primarily as a set of operational duties to be executed. Deontic expressions reinforcing obligation are equally prominent, with formulations such as "must be retained," "are required to," and "is legally bound to comply" anchoring participant responses within the normative framework of Law No. 18-07 and Law No. 25-11.

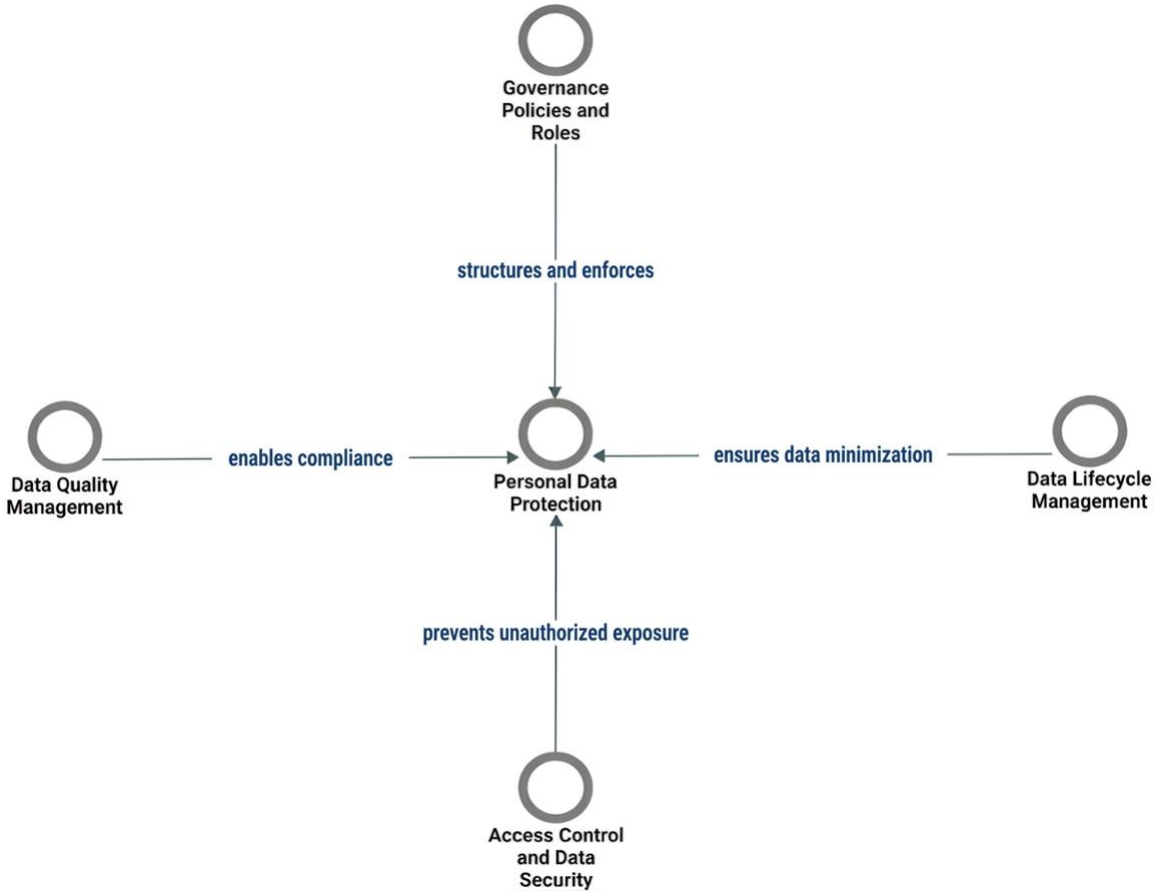
Epistemic hedging appears selectively, most notably in responses to Q6 where participants estimate policy implementation rates using formulations such as "I would estimate approximately 80%" and "approximately 90%," contrasting with the HR Officer's unhedged assertion of 100%, reflecting either greater confidence in departmental oversight or a narrower scope of assessment. First-person constructions are used most consistently by the DPO, whose dual role is reflected in formulations such as "I personally hold responsibility," indicating stronger individual identification with governance outcomes. The remaining participants, namely the IS Project Engineer, the Legal Officer, and the HR Officer, more frequently attribute responsibility to collective or institutional actors such as "the CISO and his team" or "the IS Division," a linguistic distancing that reflects their more peripheral position relative to formal governance functions.

Overall, the linguistic analysis reveals a corpus characterized by formal, obligation-oriented language and a shared tendency to anchor data protection within institutional structures and legal requirements, with personal engagement varying in direct proportion to each participant's proximity to governance responsibilities.

1.3.3. Cognitive Mapping

Cognitive mapping visually represents the key concepts raised by participants and the causal relationships between them, enabling the reconstruction of their perception of the subject under study. The approach follows Huff's (1990) causal cognitive mapping framework, which focuses on explicit causal relationships expressed by participants rather than statistical co-occurrence patterns. This choice is methodologically consistent with the interview guide, where Question 10 was specifically designed to elicit participants' causal reasoning about how data governance practices contribute to personal data protection at Condor. Using NVivo 15, the thematic codes derived from the coding phase were organized and connected based on the causal statements expressed by participants in their responses to Question 10. Each directed arrow in the resulting map represents a causal relationship articulated by participants, the level of convergence varying across dimensions. The concept map is presented in Figure 13 below.

Figure 13: Cognitive Map of DG Dimensions and Personal Data Protection



Source: Prepared by the author using NVivo 15.

The map reveals a convergent causal architecture in which Personal Data Protection occupies the central position as the outcome node, toward which all four data governance dimensions are directed. Four causal relationships emerge from participants' discourse:

- **Data Quality Management → Personal Data Protection** (enables compliance): Three out of four participants explicitly stated that accurate, validated, and consistent data enables the correct application of access control mechanisms and ensures compliance with the accuracy principle prescribed under Law No. 18-07 and Law No. 25-11. The IS Project Engineer further specified that data quality prevents non-compliance with applicable laws by ensuring data accuracy.
- **Access Control and Data Security → Personal Data Protection** (prevents unauthorized exposure): All four participants identified formalized access validation workflows, the principle of least privilege, and technical security controls as the primary mechanisms through which personal data is protected from unauthorized access and misuse.
- **Data Lifecycle Management → Personal Data Protection** (ensures data minimization): All four participants connected lifecycle management practices, including defined retention periods, archiving procedures, and formal deletion protocols, to the principle of data minimization, whereby only data strictly necessary for operational purposes is retained.
- **Governance Policies and Roles → Personal Data Protection** (structures and enforces): Three out of four participants described formally defined roles, disseminated policies, and structured compliance mechanisms as the organizational framework through which personal data protection obligations are operationalized and enforced. The Legal Officer further noted that clearly defined roles accelerate the application of procedures and the deployment of technical solutions.

The cognitive map confirms that participants hold a coherent and integrated causal representation of data governance, perceiving its four dimensions as complementary mechanisms each contributing in a distinct way to the effective protection of personal data in compliance with applicable Algerian legislation. The near-unanimous convergence across participants, particularly on Access Control and Data Lifecycle Management, reinforces the validity of these causal relationships as genuine organizational perceptions rather than isolated individual views.

1.3.4. Thematic Analysis

The thematic analysis was conducted using NVivo 15's matrix coding query function, which cross-references coded transcript segments against predefined thematic nodes. The resulting matrix, presented in Table 09, organizes participant responses across six themes: Access Control and Data Security, Data Lifecycle Management, Data Quality Management, Governance Policies and Roles, Personal Data Protection, and the Role of Data Governance in Personal Data Protection.

Table 09: Thematic Analysis Matrix

	Data Protection Officer	HR Officer	IS Engineer	Legal Affairs Officer
Access Control and Data Security	Access control at Condor follows a formal multi-step workflow. Employees request access through GLPI after notifying their manager. The CISO evaluates requests based on role and risk, seeking clarifications if needed, and either approves or rejects. Approved requests proceed to the DSI for final review. Access is revoked upon resignation or reassignment. Confidentiality is enforced by law, with penalties for breaches. A 2026 Data Loss Prevention project will classify data severity from C0 to C3.	Employees must complete a formal IT access request reviewed through management levels and approved by the Head of HR before final processing. Access to sensitive employee files is restricted, with documents secured after Law 18-07. The IS Division enforces no USB copying without permission and uses CCTV for physical surveillance.	Access control changes at Condor require formal requests approved by the CISO and IS Director; access roles are reviewed quarterly.	Legal Department requires manager approval and DSI review for data access; security includes policies and CCTV.

Data Lifecycle Management	Retention periods are set through inter-departmental coordination and formally declared to the ANPDP. Data is stored physically or digitally with security controls including firewalls, least privilege principles, and legal compliance per Laws 18-07 and 25-11, supported by backup and recovery plans. Archiving applies to legally required data, with deletion following formal destruction procedures for both digital and paper records.	Candidates register via the recruitment platform, accepting data processing terms. Post-interview, their data enters the SAP HR system where a profile with a unique ID is created. Data is stored digitally in SAP and physically in secured archives. Employee data is used for attendance, payroll, and status management. Inactive profiles are archived. Some data is retained indefinitely, while others are deleted per Algerian data protection rules.	Data is first entered into the Salesbuzz system upon email requests. Orders are processed per rules, POS accounts are disabled and archived when closed, and only the sales force manages commercial data deletion following their procedures.	The Legal Department manages data related to litigation, storing employee and client files digitally or on paper. Files are archived after final rulings or executed judgments. Data deletion is currently withheld due to legal obligations to retain records for judicial or regulatory requests.
Data Quality Management	Data quality ensured by audits; no unified data structure yet.	HR data quality is prioritized with zero errors via dual validation by employees and HR officers. Errors are corrected promptly, changes are traceable, and staff report issues through authorized personnel.	Data quality is ensured via audits; issues are detected by various teams or users and resolved internally or escalated through GLPI if needed.	Legal department relies on data originators for quality; errors are reported but not corrected by Legal.
Governance Policies and Roles	No formal data steward oversees data quality; ownership and access control are shared among senior roles (Business Process Officer, CISO, DSI). The DBA acts as data custodian with support. The Data Protection Officer ensures compliance. About 80% of data policies are followed, promoted via training, emails, and intranet.	HR data quality is a shared responsibility with joint ownership by HR Head and DSI; IS Division manages databases, compliance ensured by a cross-functional commission; policies are fully enforced with disciplinary actions.	Data quality is overseen by auditors; access control and data ownership by system admins and Business Process Owner; data storage managed by DBA; CISO ensures data protection compliance. About 90% of data policies are followed. Employee awareness is maintained via emails, sessions, and posted policies.	Data quality is ensured by originating services; Legal Manager and IS Division manage access. IS Division handles storage; CISO acts as DPO. About 80% of data policies are followed, with employees trained on them.

Personal Data Protection	Personal data includes identifiable information like birth dates and ID documents. Knowledge of data protection was gained through professional training. Data protection compliance is monitored via KPIs and audits; Condor has had no data incidents so far. Key challenges include employee resistance to secure communication methods and human error. The organization has an incident response plan involving stakeholder notification, severity assessment, resolution within seven days for serious cases, corrective actions, and formal reporting.	Personal data includes identifiable information like names and photos. Awareness and training on Law 18-07 were conducted across all divisions of Condor Electronics. Compliance is ensured via audits. The main challenge is employee resistance and lack of awareness. No incidents occurred so far; in case of a breach, the CISO leads response efforts, assessing severity and notifying relevant parties.	Personal data must be kept confidential and only shared with consent, secured by employees, and not disclosed externally. Knowledge of data protection stems from formal training and guidance from an IT Governance Manager. The CISO and cybersecurity team oversee compliance and security. Key threats include cyberattacks, information leaks, and human error. Incident response prioritizes loss minimization, prompt reporting, and resolution by the cybersecurity team.	Personal data identifies individuals and is protected under Laws 18-07 and 25-11. Compliance involves technical controls by the IS Division and supervisors in departments. Challenges include employee non-compliance and errors. Incidents must be minimized and reported promptly.
The Role of Data Governance	Condor's data governance protects personal data through access management policies limiting access to authorized users, data quality controls ensuring accurate and consistent data for effective access enforcement, and data lifecycle management that minimizes data collection to necessary purposes.	Security practices limit data access; policies and lifecycle management ensure compliance and minimize data use.	Current data governance protects personal data through data quality management, access control, internal policies, security against cyber threats, and data lifecycle management to ensure compliance and safeguard individual rights.	Data quality, security controls, data policies, lifecycle management, and defined roles ensure compliance with laws and data protection.

Source: Prepared by the author using NVivo 15.

- **Access Control and Data Security**

All four participants confirmed that access control at Condor is managed through a formal multi-step request process involving managerial approval, CISO assessment, and DSI validation, with access revoked upon departure or reassignment. The DPO provided the most detailed account, while the HR Officer added a behavioral dimension absent from other responses, noting that Law 18-07 produced a concrete change in practice, with sensitive physical files now locked in restricted archive rooms where they were previously left unsecured. The IS Engineer's contribution was the briefest, limited to confirming the formal request process and a quarterly access role review, while the Legal Affairs Officer described

- **Data Lifecycle Management**

Lifecycle management produced the most significant governance divergence across participants. The DPO described a comprehensive cycle covering acquisition, storage, processing, archiving, and deletion, with retention periods determined through inter-departmental coordination and formally declared to the ANPDP. The HR Officer provided a parallel account specific to employee data, describing consent-based acquisition, dual-format storage in SAP and secured physical archives, and deletion governed by ANPDP-stipulated periods, with certain categories such as payroll records retained indefinitely to safeguard employee rights. The IS Engineer's account was the most operationally narrow, reflecting a commercial data context where deletion responsibility falls entirely on the sales force. The most analytically significant response came from the Legal Affairs Officer, who explicitly stated that the Legal Department does not currently delete data, citing the possibility of judicial or regulatory demands for historical records at any time, a documented deviation from the data minimization requirements of Laws No. 18-07 and 25-11.

- **Data Quality Management**

Data quality management revealed the widest variation in maturity across participants. The HR Officer described the most rigorous practice, applying a zero-error standard with dual validation at the point of acquisition and full traceability of modifications. The DPO acknowledged quality is maintained through audits but noted the absence of a standardized data structure across departments and the lack of a formally designated data steward. The IS Engineer described a reactive model where issues are detected by multiple actors and resolved internally or escalated through GLPI. The Legal Affairs Officer described the most passive arrangement, where quality is entirely the responsibility of the originating department, with the Legal Department playing no corrective role. These accounts suggest

that data quality governance at Condor is decentralized and inconsistent, with maturity varying significantly by department.

- **Governance Policies and Roles**

Across all four participants, governance responsibilities are distributed rather than centralized, with the CISO functioning as the de facto anchor of data protection compliance across departments. No participant described a formally designated data steward, and role boundaries appear to be understood through practice rather than formalized documentation. Self-reported policy implementation rates varied from 80% among the DPO and Legal Officer, to 90% from the IS Engineer, to 100% from the HR Officer, a spread that likely reflects differences in departmental oversight scope rather than objective measurement. The HR Officer was alone in reporting that non-compliance carries disciplinary consequences up to and including dismissal, suggesting that enforcement stringency also varies by department.

- **Personal Data Protection**

All four participants demonstrated a working understanding of personal data as defined under Law 18-07. Three participants identified human factors, specifically resistance to change, insufficient awareness, and human error, as the primary challenges to effective protection. The DPO was the only participant to describe a fully structured incident response plan with defined severity thresholds and a seven-day resolution requirement for high-severity cases, while the HR Officer and IS Engineer deferred incident management to the CISO without describing a structured procedure. No participant reported any personal data incident to date, meaning the response framework has not been operationally validated.

- **The Role of Data Governance**

This theme produced the most direct responses to the study's central research question. All four participants articulated a causal link between data governance practices and personal data protection, though with varying depth. The DPO offered the most analytically grounded account, identifying three specific mechanisms: access management restricting data to authorized personnel, data quality controls enabling access rules to function correctly through consistent data entry, and lifecycle management enforcing data minimization. The HR Officer and Legal Affairs Officer provided convergent but less detailed responses, pointing to security practices, formal policies, and lifecycle management as the main channels. The IS Engineer offered the most comprehensive list among non-specialist roles,

identifying five contributions including security against external cyber threats, which no other participant raised. Taken together, participant responses confirm that data governance at Condor is understood as a multidimensional contributor to personal data protection, with access control and lifecycle management identified as the most consistent mechanisms across all four accounts.

2. Quantitative Results

The quantitative strand of this study employed a structured questionnaire administered to Condor Electronics' Information Systems (IS) Division personnel. The following analysis presents results from 67 valid responses, representing an 83.8% response rate from the target population of 80 employees. The analysis proceeds through descriptive statistics of the sample, reliability assessment of the instrument, and hypothesis testing to examine the relationship between data governance practices and personal data protection.

2.1. Descriptive Statistics of the Sample

This section presents the demographic characteristics of the study sample, comprising 67 valid respondents from the IS Division. The analysis examines gender distribution, age composition, educational attainment, and work experience to establish the sample profile and inform subsequent interpretation of data governance and personal data protection findings.

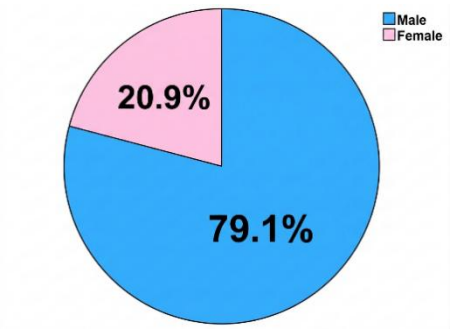
2.1.1. Gender

The gender distribution of respondents provides a basic demographic characteristic of the sample composition within the division. This descriptive information contributes to understanding the overall profile of personnel involved in the organization's information systems operations. The gender distribution of the study sample is presented below:

Table 10: Gender Distribution of Study Sample

Gender	Frequency	Percent
Male	53	79.1
Female	14	20.9
Total	**67**	**100.0**

Figure 14: Gender Distribution of Study Sample



Source: Prepared by the author using SPSS Statistics 31.

The sample demonstrates a predominantly male composition, with 53 male respondents representing 79.1% of the total sample, compared to 14 female respondents accounting for 20.9%. This gender distribution reflects the typical demographic pattern observed in information systems and technology-related divisions, where male employees constitute the majority of the workforce. The pronounced gender imbalance indicates that the study findings are primarily informed by male perspectives within the division.

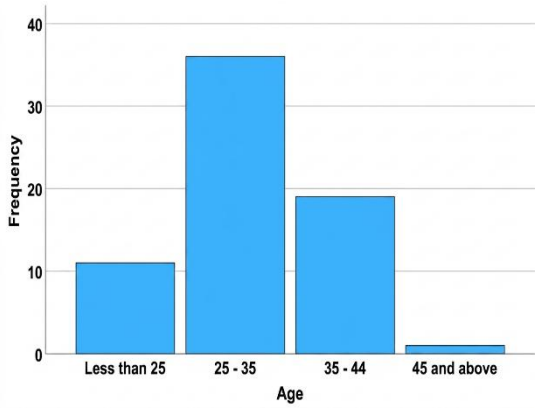
2.1.2. Age

Age distribution within the workforce can reflect the experience profile and generational composition of personnel in the IS Division. Understanding the age structure of respondents provides insight into the demographic maturity of the sample and contributes to characterizing the professional context within which data governance practices are implemented at Condor Electronics. The age distribution of the study sample is illustrated as follows:

Table 11: Age Distribution of Study Sample

Age Group	Frequency	Percent
Less than 25	11	16.4
25 - 35	36	53.7
35 - 44	19	28.4
45 and above	1	1.5
Total	**67**	**100.0**

Figure 15: Age Distribution of Study Sample



Source: Prepared by the author using SPSS Statistics 31.

The age distribution reveals a predominantly young to middle-aged workforce, with the majority of respondents (36 individuals, 53.7%) falling within the 25-35 age range. The second largest group comprises employees aged 35-44 years (19 respondents, 28.4%), while younger employees under 25 years represent 16.4% of the sample (11 respondents). Notably, employees aged 45 and above constitute only 1.5% of the sample with a single respondent, indicating a markedly young demographic profile within the division. This age structure suggests a workforce characterized by early to mid-career professionals with relatively limited representation of senior-aged personnel.

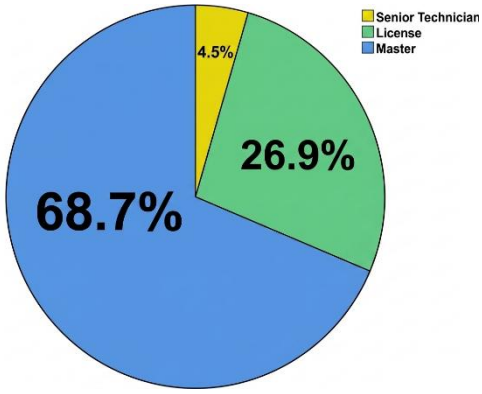
2.1.3. Education Level

Educational attainment represents a key demographic characteristic that can influence employees' understanding of data governance principles and their capacity to implement personal data protection measures. Within the IS Division, the distribution of academic qualifications may reflect the technical and regulatory competence available to support compliance with data protection requirements. The education level composition of the study sample is presented below:

Table 12: Sample Education Profile

Education Level	Frequency	Percent
Senior Technician	3	4.5
License	18	26.9
Master	46	68.7
Total	**67**	**100.0**

Figure 16: Sample Education Profile



Source: Prepared by the author using SPSS Statistics 31.

The education level distribution indicates a highly qualified workforce within the IS Division. The majority of respondents hold a master's degree, with 46 individuals representing 68.7% of the total sample. The second largest group comprises employees with a License degree, accounting for 18 respondents (26.9%). A small minority of participants possess a Senior Technician qualification, with 3 respondents (4.5%). No other educational categories were reported among the sample. This educational profile suggests that the division is staffed predominantly by personnel with advanced university degrees, which may positively influence the understanding and implementation of data governance frameworks and personal data protection practices requiring specialized knowledge and analytical capabilities.

2.1.4. Work Experience

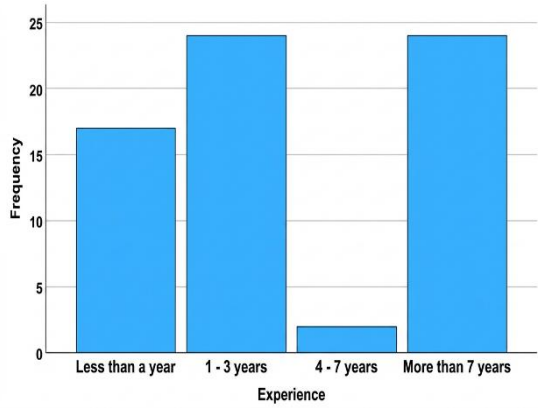
Work experience reflects the accumulated practical knowledge and familiarity that employees bring to their roles within the division. The length of time personnel have spent in the workforce or within similar functions can influence their exposure to data handling practices, organizational procedures, and evolving data protection standards. Understanding

the experience profile of respondents provides context for interpreting perceptions of data governance and personal data protection outcomes at Condor Electronics. The work experience distribution of the study sample is presented below:

Table 13: Sample Experience Profile

Experience Level	Frequency	Percent
Less than a year	17	25.4
1 - 3 years	24	35.8
4 - 7 years	2	3.0
More than 7 years	24	35.8
Total	**67**	**100.0**

Figure 17: Sample Experience Profile



Source: Prepared by the author using SPSS Statistics 31.

The work experience distribution across the 67 respondents reveals a predominantly early-career profile, with the largest groups being those with 1–3 years of experience and those with more than 7 years, each accounting for 35.8% of the sample. Respondents with less than one year of experience represent 25.4%, while those in the 4–7 year range constitute a marginal 3.0%. This distribution indicates that the majority of the workforce within the division is composed of either relatively recent recruits or long-tenured employees, with limited representation of mid-career staff. As a result, the study findings reflect perspectives shaped by either early-stage professional exposure or extended organizational experience, with little contribution from the intermediate experience bracket.

2.2. Reliability Test (Cronbach's Alpha)

Prior to conducting the main statistical analyses, the internal consistency of the measurement instrument was assessed using Cronbach's alpha coefficient. This reliability test was applied to both the independent variable scale (Data Governance) and the dependent variable scale (Personal Data Protection), as well as to the full instrument, in order to verify that the items within each scale consistently measure their intended constructs. A threshold of $\alpha \geq 0.70$ is generally accepted as indicative of satisfactory reliability in social science research (Nunnally, 1978).

Table 14: Reliability Analysis of the Research Instrument

Reliability Statistics

Variables	Cronbach's Alpha	N of items
Data Governance	.909	16
Personal Data Protection	.884	14
Total	**.931**	**30**

Source: Prepared by the author using SPSS Statistics 31.

The reliability analysis yields satisfactory to excellent internal consistency coefficients across all scales. The full instrument attains an alpha of 0.931, indicating a high degree of overall coherence among the 30 items. The Data Governance scale records an alpha of 0.909, and the Personal Data Protection scale returns a value of 0.884, both of which comfortably exceed the accepted threshold and confirm that each scale reliably measures its respective construct. These results support the suitability of the instrument for subsequent correlation and regression analyses. For full reliability results, see Appendix E.

2.3. Likert Scale Categories

To determine the cell width of the Likert scale intervals used in this study, the following formula was applied: cell width = (maximum value − minimum value) ÷ number of categories = (5 − 1) ÷ 5 = 0.80. This value was then added to the minimum value of the scale to establish the lower boundary of each interval. The resulting intervals and their corresponding interpretations are presented in Table 15 below.

Table 15: Likert Scale Category Boundaries

Interval	Interpretation
[1.00 – 1.80[	Strongly Disagree
[1.80 – 2.60[	Disagree
[2.60 – 3.40[	Neutral
[3.40 – 4.20[	Agree
[4.20 – 5.00]	Strongly Agree

Source: Prepared by the author.

2.4. Descriptive Analysis of Variables

The following table presents the descriptive statistics for each study variable, including the mean score, standard deviation, and corresponding Likert scale interpretation for all 67 respondents.

Table 16: Descriptive Statistics of Study Variables

Dimension	N	Mean	Std. Deviation	Interpretation
Data Quality Management (DQM)	67	4.12	0.855	Agree
Access Control and Security (ACS)	67	4.46	0.696	Strongly Agree
Data Lifecycle Management (DLM)	67	4.11	0.680	Agree
Governance Policies and Roles (GPR)	67	4.18	0.641	Agree
Data Governance (DG)	67	4.22	0.592	Strongly Agree
Personal Data Protection (PDP)	67	4.17	0.564	Agree

Source: Prepared by the author using SPSS Statistics 31.

The descriptive analysis of the study variables reveals consistently positive perceptions across all dimensions among IS Division employees at Condor Electronics. Access Control and Security recorded the highest mean score among the data governance sub-dimensions (M = 4.46, SD = 0.696), falling within the Strongly Agree interval, indicating that access-related practices are the most consistently perceived and applied across the division. The relatively low standard deviation further suggests that employee perceptions on this dimension are largely uniform, with little disagreement across respondents. Data Quality Management recorded a mean of 4.12 (SD = 0.855), falling within the Agree interval, however its standard deviation is the highest among all dimensions, indicating notable variability in how employees perceive data quality practices, suggesting that this area may be experienced differently depending on the respondent's role or department within the division. Data Lifecycle Management (M = 4.11, SD = 0.680) and Governance Policies and Roles (M = 4.18, SD = 0.641) both fall within the Agree interval with relatively low standard deviations, reflecting not only positive but also broadly consistent perceptions across respondents regarding lifecycle and compliance-related practices. At the composite level, the overall Data Governance mean (M = 4.22, SD = 0.592) falls within the Strongly Agree interval with the lowest standard deviation among all dimensions, indicating that when

governance is considered as a whole, employee perceptions converge most strongly around a positive assessment. The Personal Data Protection variable recorded a mean of 4.17 (SD = 0.564), falling within the Agree interval with a similarly low standard deviation, suggesting broad consensus among employees regarding personal data protection outcomes. See Appendix E for item-level means and standard deviations.

It should be noted that these scores reflect employee perceptions of data handling practices and must be read in conjunction with the qualitative findings presented in Section 1 and the discussion that follows in Section 2 of this chapter.

2.5. Statistical Assumptions

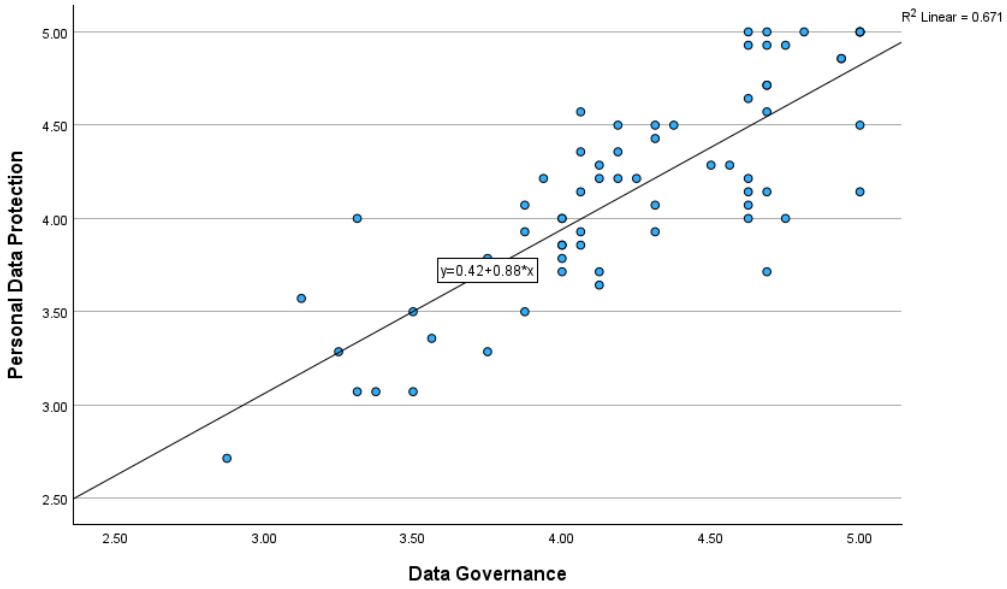
Before conducting the main statistical analyses, the assumptions underlying simple and multiple linear regression, followed by Pearson correlation, were examined to ensure the validity and interpretability of the results. The following sub-sections present the diagnostic tests applied for each analysis.

2.5.1. Assumptions of Simple Linear Regression

One extreme outlier was identified in the dataset through residual diagnostics. Its residual value deviated substantially from the distribution of all other observations and was determined to be sufficiently influential to compromise the integrity of the model, justifying its exclusion (Tabachnick & Fidell, 2013). All subsequent regression analyses were therefore conducted on a final analytical sample of n = 66.

Linearity was assessed through a scatterplot of the Data Governance composite mean against the Personal Data Protection composite mean. As illustrated in Figure 18, the data points distribute along a discernible linear trajectory with no evidence of curvature or systematic departure from linearity. The linear fit line ($y = 0.42 + 0.88x$, $R^2 = 0.671$) confirms that the relationship between the two variables is adequately captured by a linear model. The linearity assumption is therefore considered satisfied.

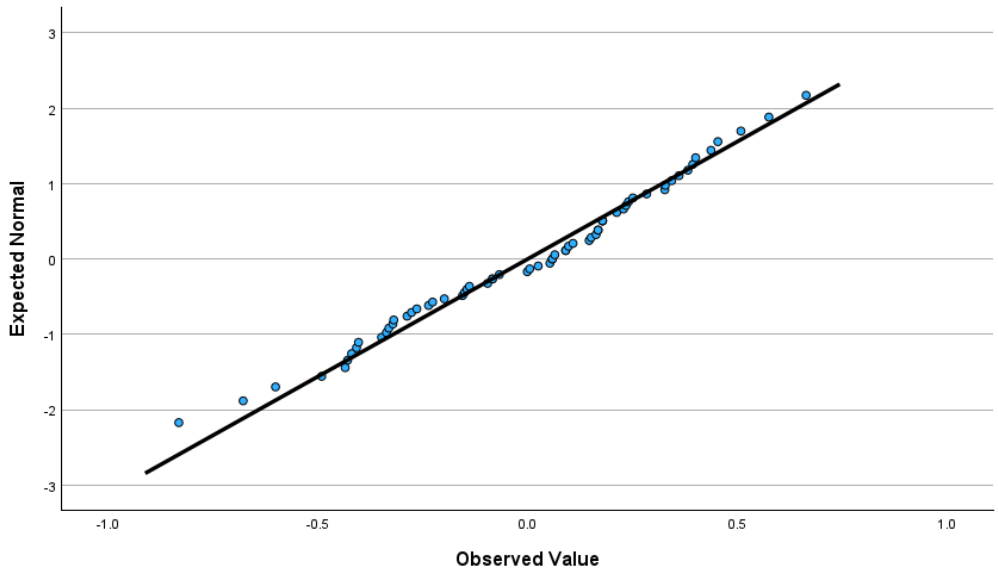
Figure 18: Scatterplot of Data Governance and Personal Data Protection



Source: Prepared by the author using SPSS Statistics 31.

Normality of residuals was assessed through both visual inspection and formal statistical testing. As Field (2013) and Hair et al. (2019) note, the normality assumption in linear regression applies to the residuals of the model rather than to the raw variables themselves. The Q-Q plot revealed that the observed values follow the diagonal reference line closely throughout with no substantial deviation, providing visual confirmation of normality.

Figure 19: Normal Q-Q Plot of Unstandardized Residuals



Source: Prepared by the author using SPSS Statistics 31.

This was further confirmed by the Tests of Normality presented in the table below.

Table 17: Tests of Normality for Unstandardized Residuals

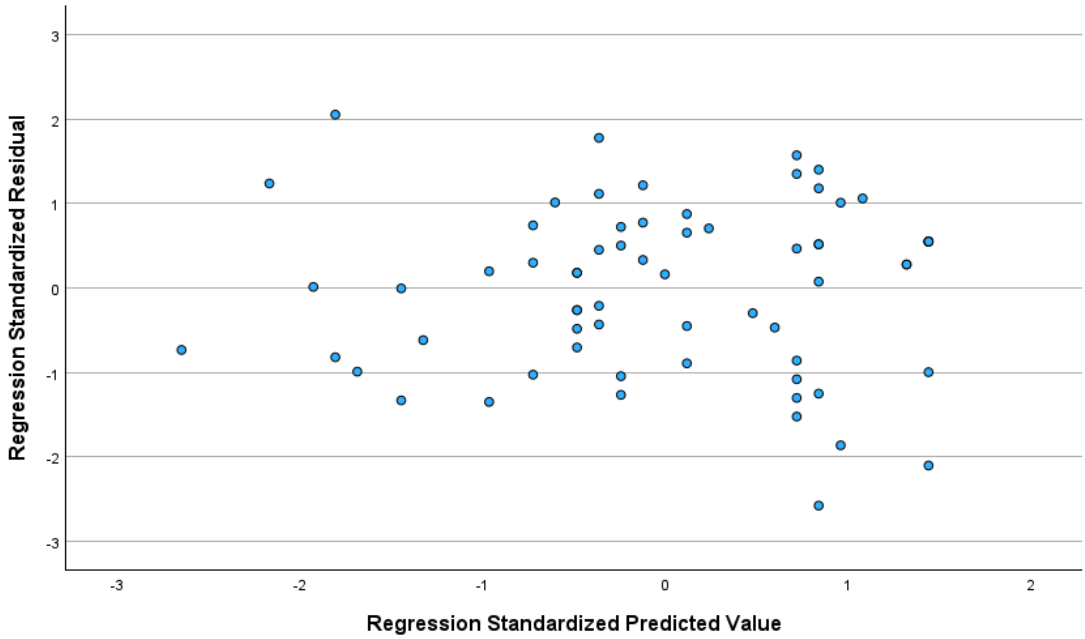
	Kolmogorov-Smirnov			Shapiro-Wilk		
	Statistic	**df**	**Sig.**	**Statistic**	**df**	**Sig.**
Unstandardized Residual	.096	66	.200	.983	66	.503

Source: Prepared by the author using SPSS Statistics 31.

Both the Kolmogorov-Smirnov ($p = .200$) and Shapiro-Wilk ($W = 0.983$, $p = .503$) tests returned significance values above the 0.05 threshold, confirming that the residuals are normally distributed and that the normality assumption is fully satisfied.

Homoscedasticity was assessed through the standardized residuals scatterplot. The points are distributed randomly around zero with no discernible systematic pattern, confirming that the variance of the residuals is approximately constant across all predicted values. All regression assumptions are therefore considered satisfactorily met.

Figure 20: Residuals Scatterplot



Source: Prepared by the author using SPSS Statistics 31.

2.5.2. Multicollinearity Diagnostics (VIF)

Prior to interpreting the multiple regression results, multicollinearity among the four predictors was assessed through the Variance Inflation Factor. Multicollinearity occurs when

independent variables are highly correlated with one another, inflating standard errors and rendering individual coefficient estimates unreliable. A VIF value below 5 is generally considered acceptable in social science research (O'brien, 2007).

Table 18: Collinearity Statistics

Variable	Tolerance	VIF
Data Quality Management	.620	1.613
Access Control and Security	.556	1.797
Data Lifecycle Management	.584	1.712
Governance Policies and Roles	.445	2.247

Source: Prepared by the author using SPSS Statistics 31.

All four predictors returned VIF values well below the threshold of 5, ranging from 1.613 for Data Quality Management to 2.247 for Governance Policies and Roles. These values confirm the absence of multicollinearity among the independent variables, indicating that each sub-dimension contributes sufficiently distinct information to the model and that the regression coefficients can be interpreted with confidence.

2.5.3. Assumptions of Pearson Correlation

Pearson correlation requires that the relationship between the variables is linear and that no extreme outliers distort the correlation coefficient. Linearity was assessed through a scatterplot, which confirmed a clear linear trajectory between Data Governance and Personal Data Protection (Figure 18). One extreme outlier identified through residual diagnostics was removed prior to analysis, resulting in a final sample of N = 66. To satisfy the interval data requirement, composite scores were calculated using the mean of the Likert items for each construct. While Pearson's *r* formally assumes bivariate normality for significance testing, the analysis relied on the Central Limit Theorem, which ensures that the sampling distribution approaches normality at moderate sample sizes (N > 30). As Field (2013) notes, the test is robust to violations of marginal distributions under these conditions. Both primary assumptions were therefore considered satisfactorily met.

2.6. Hypotheses Testing

In order to determine the validity of the hypotheses, the significance level (Sig.) resulting from the statistical tests is examined. Two competing hypotheses are considered for each test:

- **H_0 (Null Hypothesis):** There is no statistically significant effect of data governance practices on personal data protection at Condor Electronics.
- **H_1 (Alternative Hypothesis):** There is a statistically significant effect of data governance practices on personal data protection at Condor Electronics, indicating a meaningful relationship between the two variables.

If the significance level (Sig.) is less than or equal to 0.05, the null hypothesis is rejected and the alternative hypothesis is accepted. If the significance value exceeds 0.05, the null hypothesis is retained.

2.6.1. Simple Linear Regression

The regression analysis was conducted with Data Governance as the independent variable and Personal Data Protection as the dependent variable, based on the cleaned sample of n = 66. The results are presented in the tables below.

Table 19: Model Summary for Simple Linear Regression

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.819[a]	.671	.665	.32332

Source: Prepared by the author using SPSS Statistics 31.

The Model Summary table shows that the regression model produced a correlation coefficient of R = 0.819, indicating a strong positive relationship between data governance and personal data protection. The coefficient of determination $R^2 = 0.671$ indicates that 67.1% of the variance in personal data protection scores is explained by data governance practices, while the Adjusted $R^2 = 0.665$ confirms that this result is stable and accounts for the sample size.

Table 20: ANOVA Summary for Simple Linear Regression

Model		Sum of Squares	df	Mean Square	F	Sig.
1	**Regression**	13.621	1	13.621	130.300	<.001[b]
	Residual	6.690	64	.105		
	Total	20.312	65			

Source: Prepared by the author using SPSS Statistics 31.

The ANOVA table confirms that the overall regression model is statistically significant ($F = 130.300$, $p < .001$), meaning that data governance is a significant predictor of personal data protection and that the model explains a substantial portion of the variance in the dependent variable.

Table 21: Coefficients Results for Simple Linear Regression

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	**(Constant)**	.420	.330		1.271	.208
	DG_Mean	.880	.077	.819	11.415	<.001

Source: Prepared by the author using SPSS Statistics 31.

The data governance coefficient ($B = 0.880$, $p < .001$) is statistically significant, indicating that for every one-unit increase in the data governance composite score, the personal data protection score increases by 0.880 units on average. The standardized coefficient Beta = 0.819 further confirms the strength and direction of this relationship. The regression equation is expressed as follows:

$$\mathbf{PDP = 0.420 + 0.880 \times DG}$$

Since the significance value ($p < .001$) falls below the 0.05 threshold, the null hypothesis is rejected and the alternative hypothesis is accepted. Data governance practices at Condor Electronics exert a statistically significant and strong positive effect on personal data protection, providing empirical support for the study's central argument.

2.6.2. Multiple Linear Regression

To examine the independent contribution of each data governance sub-dimension to personal data protection outcomes, a multiple linear regression was conducted with the four sub-dimensions entered simultaneously as independent variables and Personal Data Protection as the dependent variable, based on the cleaned sample of n = 66. The results are presented in the tables below.

Table 22: Model Summary for Multiple Linear Regression

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.839[a]	.704	.685	.31386

Source: Prepared by the author using SPSS Statistics 31.

The multiple regression model produced a correlation coefficient of R = 0.839, indicating a strong positive relationship between the four data governance sub-dimensions collectively and personal data protection. The coefficient of determination $R^2 = 0.704$ indicates that 70.4% of the variance in personal data protection scores is explained by the four sub-dimensions combined, while the Adjusted $R^2 = 0.685$ confirms that this result remains robust after accounting for the number of predictors and the sample size. Compared to the simple linear regression model ($R^2 = 0.671$), the multiple regression model accounts for an additional 3.3% of variance, reflecting the added explanatory value of disaggregating data governance into its constituent dimensions.

Table 23: ANOVA Summary for Multiple Linear Regression

	Model	Sum of Squares	df	Mean Square	F	Sig.
1	**Regression**	14.303	4	3.576	36.299	<.001[b]
	Residual	6.009	61	.099		
	Total	20.312	65			

Source: Prepared by the author using SPSS Statistics 31.

The ANOVA table confirms that the overall multiple regression model is statistically significant ($F = 36.299$, $p < .001$), establishing that the four data governance sub-dimensions jointly constitute a significant and meaningful predictor set for personal data protection outcomes.

Table 24: Coefficients Results for Multiple Linear Regression

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	**Std. Error**	**Beta**	**t**	**Sig.**
1	**(Constant)**	.150	.349		.430	.669
	Data Quality Management	.075	.062	.107	1.211	.230
	Access Control and Security	.277	.095	.273	2.925	.005
	Data Lifecycle Management	.326	.090	.330	3.617	<.001
	Governance Policies and Roles	.262	.090	.303	2.900	.005

Source: Prepared by the author using SPSS Statistics 31.

The coefficients table reveals important distinctions in the independent contribution of each sub-dimension to personal data protection outcomes when all four are considered simultaneously. Data Lifecycle Management emerges as the strongest individual predictor (B = 0.326, Beta = 0.330, $p < .001$), indicating that structured approaches to data retention, backup, and secure disposal exert the most direct independent effect on personal data protection among all sub-dimensions. Governance Policies and Roles constitutes the second strongest predictor (B = 0.262, Beta = 0.303, $p = .005$), confirming that legal compliance awareness and employee training independently contribute to personal data protection outcomes beyond what is explained by the other dimensions. Access Control and Security registers as the third significant predictor (B = 0.277, Beta = 0.273, $p = .005$), reflecting the independent protective effect of structured access governance. Data Quality Management, however, does not reach statistical significance in the multiple regression model (B = 0.075, Beta = 0.107, $p = .230$), indicating that when the shared variance among all four sub-dimensions is accounted for, data quality management does not independently predict personal data protection outcomes. This finding does not contradict the Pearson correlation result for Data Quality Management ($r = 0.563$, $p < .001$), which reflects its bivariate relationship with personal data protection; rather, it suggests that its contribution is largely mediated through its overlap with the other three dimensions, particularly Governance Policies and Roles with which it shares the highest inter-predictor correlation ($r = 0.589$).

The multiple regression equation can therefore be expressed as follows:

$$\mathbf{PDP = 0.150 + 0.075(DQM) + 0.277(ACS) + 0.326(DLM) + 0.262(GPR)}$$

2.6.3. Pearson Correlation Analysis

Pearson correlation analysis was conducted to examine the strength and direction of the relationship between each data governance sub-dimension and personal data protection, enabling the testing of the four sub-hypotheses. For each sub-hypothesis, the null hypothesis (H_0) states that no statistically significant relationship exists between the sub-dimension and personal data protection, while the alternative hypothesis (H_1) states that a statistically significant relationship does exist. If the significance value is less than or equal to 0.05, H_0 is rejected and H_1 is accepted.

Table 25: Pearson Correlation Matrix

	DQM	ACS	DLM	GPR	PDP
DQM	1	.503***	.426***	.589***	.563***
ACS	.503***	1	.537***	.615***	.690***
DLM	.426***	.537***	1	.610***	.707***
GPR	.589***	.615***	.610***	1	.735***
PDP	.563***	.690***	.707***	.735***	1

Source: Prepared by the author using SPSS Statistics 31.

- **Sub-Hypothesis 1: Data Quality Management**

The Pearson correlation between Data Quality Management and Personal Data Protection yielded $r = 0.563$ ($p < .001$). Since the significance value is below the 0.05 threshold, the null hypothesis is rejected and the alternative hypothesis is accepted. A statistically significant moderate positive relationship exists between data quality management practices and personal data protection outcomes at Condor Electronics. The moderate strength of this correlation, while still significant, is the weakest among the four sub-dimensions and is analytically consistent with the absence of formal data quality policies identified in the documentary analysis. It suggests that while employees perceive data quality practices as contributing to personal data protection, this contribution is less direct and less institutionally anchored than that of the other governance dimensions, reflecting the ad hoc nature of data quality management at Condor Electronics.

- **Sub-Hypothesis 2: Access Control and Security**

The Pearson correlation between Access Control and Security and Personal Data Protection yielded r = 0.690 (p < .001). The significance value is below the 0.05 threshold, leading to the rejection of the null hypothesis and the acceptance of the alternative hypothesis. A statistically significant strong positive relationship exists between access control practices and personal data protection outcomes, indicating that structured access governance, including need-to-know provisioning, account lifecycle management, and technical security controls, contributes strongly to employees' perception of personal data protection within the organization. This strong correlation is consistent with access control being the most elaborately documented governance dimension across the policy corpus, suggesting that its operational elaborateness does translate into meaningful personal data protection outcomes at the employee perception level.

- **Sub-Hypothesis 3: Data Lifecycle Management**

The Pearson correlation between Data Lifecycle Management and Personal Data Protection yielded r = 0.707 (p < .001). The significance value falls below the 0.05 threshold, resulting in the rejection of the null hypothesis and the acceptance of the alternative hypothesis. A statistically significant strong positive relationship exists between data lifecycle management practices and personal data protection outcomes, indicating that structured approaches to data retention, backup, archiving, and secure disposal have a strong and direct bearing on how well personal data is protected throughout its operational life within the organization. The strength of this correlation suggests that employees perceive lifecycle management practices as among the most tangible and directly relevant governance mechanisms for personal data protection in their daily work.

- **Sub-Hypothesis 4: Governance Policies and Roles**

The Pearson correlation between Governance Policies and Roles and Personal Data Protection yielded r = 0.735 (p < .001). The significance value is below the 0.05 threshold, leading to the rejection of the null hypothesis and the acceptance of the alternative hypothesis. A statistically significant strong positive relationship exists between governance policy and role assignment practices and personal data protection outcomes, with this dimension recording the highest correlation among all four sub-dimensions. This indicates that legal compliance awareness, policy dissemination, and employee training are the governance practices most strongly and directly associated with personal data protection outcomes at Condor Electronics, suggesting that embedding personal data protection

obligations within a formal compliance culture has the most measurable impact on protection outcomes among all governance dimensions examined. This finding is consistent with the documentary analysis, which identified legal and regulatory compliance as the most cross-cutting theme across the policy corpus.

Table 26: Summary of Hypotheses Testing Results

Hypothesis	Statistical Test	Result	Decision
Main: DG significantly contributes to PDP	Regression ($R = 0.819$, $R^2 = 0.671$, Adjusted $R^2 = 0.665$)	$F = 130.300$, $p < .001$	H_0 Rejected
H1: DQM has significant relationship with PDP	Pearson ($r = 0.563$)	$p < .001$	H_0 Rejected
H2: ACS has significant relationship with PDP	Pearson ($r = 0.690$)	$p < .001$	H_0 Rejected
H3: DLM has significant relationship with PDP	Pearson ($r = 0.707$)	$p < .001$	H_0 Rejected
H4: GPR has significant relationship with PDP	Pearson ($r = 0.735$)	$p < .001$	H_0 Rejected

Source: Prepared by the author using SPSS Statistics 31.

Section 2: Discussion

This section synthesizes and interprets the empirical findings presented in the preceding results section, drawing on the full body of evidence collected through field observation, documentary analysis, semi-structured interviews, and the administered questionnaire. Rather than restating the findings, the discussion situates them within the study's theoretical framework, examines their implications for data governance and personal data protection at Condor Electronics, and considers their broader significance in light of the existing literature.

1. Discussion of Research Questions and Problem Statement

The following sub-section addresses each of the study's four research questions through a systematic triangulation of findings drawn from field observation, documentary analysis, semi-structured interviews, and questionnaire data. Each question is examined against the

full body of evidence collected, with the aim of producing interpretations that are grounded in convergent findings across multiple sources rather than in any single data strand alone.

- **RQ1: To what extent does Condor Electronics implement data governance practices?**

Triangulating findings across all four data sources reveals a consistent and coherent picture: data governance practices exist at Condor Electronics at the operational level, but their implementation is partial, fragmented, and structurally unsupported by a unified governance framework. Observation confirmed the presence of governance policies in both digital and physical form within the IS Division, the active use of GLPI as a formalized internal tool for access requests and issue reporting, and recurring data awareness sessions for new employees. Documentary analysis identified nine ISO 27001:2022-aligned policy documents covering access control, data lifecycle management, information classification, and regulatory compliance, demonstrating that governance-related provisions are formally documented across multiple domains. Interview data further confirmed that formal data-handling policies are in place and disseminated through training sessions, internal communications, and intranet publication, with implementation rates estimated at 80% by the CISO, 90% by the IS Project Engineer, and 100% within the HR Department by the HR Officer. The questionnaire results are consistent with these estimates, producing an overall Data Governance mean of 4.22 (SD = 0.592), falling within the Strongly Agree interval, reflecting broadly positive employee perceptions of governance practice across all four sub-dimensions.

However, these positive indicators must be interpreted within the structural reality identified across the qualitative strand. No unified data governance framework exists at the organizational level, governance roles are informally distributed and referenced by job title rather than formally defined governance responsibilities, the data steward role is absent, and the IT Standards and Governance Manager position (the closest institutional approximation to a formal governance function) has remained vacant since its removal in 2023. Documentary analysis further revealed the complete absence of any data quality management policy across the nine documents examined, indicating that governance efforts have been directed primarily toward security, compliance, and access control while data quality as an organizational asset remains unaddressed at the policy level. These structural gaps are consistent with the characterization of Condor Electronics as a low governance maturity organization, where practices exist and are perceived positively by employees but

operate in an ad hoc and fragmented manner rather than as part of a systematic, monitored, and accountable governance architecture. This finding is consistent with the DAMA-DMBOK framework's distinction between the existence of governance activities and the existence of a governance program, the former being present at Condor while the latter remains absent.

- **RQ2: How does Condor Electronics handle personal data breaches and incidents?**

This research question is addressed exclusively through the interview data, as neither observation, documentary analysis, nor the questionnaire instrument was designed to capture incident response mechanisms in operational detail. Across all four interviews, a consistent picture emerged: a formal incident response plan is in place, no personal data incidents have occurred to date within the experience of any of the four participants, and the CISO holds primary responsibility for coordinating the organization’s response to any such event.

The CISO described a structured response cycle initiated by the notification of all relevant stakeholders and the completion of an initial contact sheet recording the identities of those informed and the precise times of notification. Incidents classified as high severity must be resolved within a maximum of seven days, following deliberation by the response team on appropriate containment and remediation measures. Upon resolution, a formal incident report is prepared documenting all relevant details and the corrective measures identified to prevent recurrence. The IS Project Engineer confirmed that the first priority in any incident is to minimize losses as quickly as possible before reporting to the CISO and his cybersecurity team, while the Legal Officer described an immediate notification of the IS Division by email as the first departmental response. The HR Officer, while noting no personal experience of such an incident, confirmed that the CISO would be the primary responsible party and that the immediate response would involve assessing severity and notifying all relevant parties.

The existence of a structured incident response plan, the defined severity classification system, and the consistent attribution of response responsibility to the CISO and cybersecurity team across all four participants indicate that Condor Electronics has invested in formalizing its breach response capacity. This is consistent with the Security Incident Management Policy identified in the documentary analysis, which classifies the unauthorized disclosure of customer personal data as a distinct incident category and mandates a structured response cycle aligned with the provisions of Law No. 18-07. The

absence of any recorded personal data incident to date, while positive, should be interpreted cautiously, it may reflect genuine effectiveness of preventive controls, but it may equally reflect an absence of detection mechanisms sophisticated enough to identify all breaches.

- **RQ3: To what extent do Condor Electronics employees comply with personal data protection policies and practices?**

Evidence from both the qualitative and quantitative strands converges on a generally positive but contextually nuanced picture of employee compliance. Observation confirmed the recurring presence of data awareness sessions for new employees and the physical display of the data security policy throughout the IS Division workspace, indicating that the organization actively communicates its protection obligations to staff. The HR Officer noted that following the enactment of Law No. 18-07, a significant behavioral change occurred within the HR Department (sensitive paper documents previously handled without formal precautions are now organized and secured in a restricted-access archive room) suggesting that regulatory awareness has produced tangible compliance outcomes at the departmental level. Additionally, Condor Electronics was among the first three companies in Algeria to formally register with the ANPDP upon the introduction of Law No. 18-07, reflecting an early and proactive institutional commitment to regulatory compliance.

Interview estimates of policy implementation ranged from 80% (CISO and Legal Officer) to 90% (IS Project Engineer) to 100% within the HR Department (HR Officer), reflecting generally high but not universal compliance. The CISO identified employee resistance to using secure communication channels as a primary compliance challenge, citing the use of informal messaging applications such as WhatsApp for sharing sensitive financial data as a concrete example. Human error was identified as a persistent concern across all four participants regardless of role, indicating that behavioral compliance remains imperfect despite the technical and procedural controls in place. Quantitatively, the Governance Policies and Roles dimension recorded a mean of 4.18 (SD = 0.641), falling within the Agree interval with a low standard deviation, suggesting broadly consistent employee perceptions of policy-related governance practices. The Personal Data Protection mean of 4.17 (SD = 0.564) further reflects a generally positive assessment of protection outcomes, though as noted in the results section, these scores reflect operational behavior rather than formal governance awareness.

- **RQ4: What challenges does Condor Electronics face in protecting personal data, and how can data governance practices help overcome them?**

Four principal challenges to personal data protection were identified across the qualitative data sources. Human error emerged as the most consistently cited challenge across all four interviews, described as an ongoing concern irrespective of the technical and procedural controls in place. Employee resistance to change constituted the second challenge, manifesting most concretely in the use of informal communication channels for sharing sensitive data despite formal policies requiring secure channels. The absence of a unified data governance framework represents the third and most structurally significant challenge: without formally defined governance roles, a central coordination mechanism, or a data quality management policy, the existing practices lack the consistency and accountability necessary to systematically prevent protection failures. The vacancy of the IT Standards and Governance Manager position since 2023 crystallizes this structural gap, as it represents the deliberate removal of the only role that could have provided organization-wide governance oversight. The fourth challenge, identified through documentary analysis and confirmed by the CISO, is the risk of regulatory non-compliance in the context of cloud migration and cross-border data transfers, where the absence of a formalized data protection governance model creates legal vulnerability under Law No. 18-07 and the ANPDP authorization requirements.

Data governance practices offer a structured response to each of these challenges. Human error and resistance to change are addressed through the training and awareness mechanisms embedded in the Governance Policies and Roles dimension, whose strong correlation with personal data protection outcomes ($r = 0.735$) confirms that investment in policy dissemination and employee training produces measurable protection outcomes. The structural gap left by the absent governance framework is addressed directly by the DAMA-DMBOK recommendation for a formal governance program with defined roles, documented processes, and accountability mechanisms, a recommendation that the Cloud Migration Strategy Policy itself implicitly endorses through its requirement to update the data protection governance model and define a stakeholder roles matrix. The cloud compliance risk is addressed through the access control and lifecycle management provisions already present in the policy corpus, which require ANPDP authorization for cross-border data hosting and mandate secure erasure upon service termination. The quantitative findings reinforce this picture: Data Lifecycle Management ($r = 0.707$) and Access Control and

Security (r = 0.690) both demonstrate strong relationships with personal data protection, confirming that strengthening these dimensions would produce the most direct and measurable improvements in protection outcomes.

- **Problem Statement: How does data governance, as delivered by its practices at Condor Electronics, contribute towards personal data protection?**

The triangulated findings across all four data sources converge on a single answer: data governance at Condor Electronics contributes to personal data protection meaningfully but incompletely, through a set of operational practices that produce measurable protection outcomes despite the absence of a unified governance framework. The quantitative evidence confirms this contribution empirically, with the regression model establishing that data governance explains 67.1% of the variance in personal data protection outcomes ($R^2 = 0.671$, $F = 130.300$, $p < .001$), and the Pearson correlations confirming significant positive relationships between all four governance sub-dimensions and personal data protection. The qualitative evidence contextualizes and enriches this finding: the contribution of governance to protection is real and perceived by employees across all roles, but it operates through fragmented and informally sustained mechanisms rather than through a systematic governance architecture. Access control is the most operationally developed mechanism, lifecycle management and compliance practices are formally documented but unevenly implemented, and data quality governance (a foundational dimension of any mature governance program) remains entirely absent at the policy level. The removal of the IT Standards and Governance Manager position in 2023 represents the most concrete expression of this structural deficit, signaling that the organization has not prioritized the institutionalization of governance at the level required to fully and consistently deliver personal data protection. The answer to the main problematic is therefore not binary (governance either contributes or it does not) but graduated: current practices contribute substantially to personal data protection, and their contribution would be considerably stronger if supported by a formal, unified, and role-defined governance framework.

2. Discussion of Hypotheses

The following sub-section interprets the results of the hypothesis testing in light of the study's empirical and qualitative findings, addressing both the main hypothesis and the four sub-hypotheses.

2.1. Main Hypothesis

The regression analysis confirmed that data governance practices at Condor Electronics exert a statistically significant and strong positive effect on personal data protection (B = 0.880, $R^2 = 0.671$, F = 130.300, $p < .001$), meaning that 67.1% of the variance in personal data protection outcomes is explained by data governance practices. This result is attributable to the cumulative effect of the four governance dimensions operating together, as access control, lifecycle management, compliance practices, and policy enforcement collectively create an environment in which personal data is consistently handled, protected, and monitored. The remaining 32.9% of unexplained variance reflects factors outside the scope of the instrument, including individual attitudes, organizational culture, leadership commitment, and IT infrastructure quality, none of which were measured in this study. This finding provides strong empirical support for the main hypothesis and is consistent with the qualitative evidence, which established that governance mechanisms, however fragmented, are perceived by employees across all roles as directly contributing to personal data protection outcomes.

2.2. Sub-Hypotheses

Pearson correlation analysis confirmed statistically significant positive relationships between all four data governance sub-dimensions and personal data protection, leading to the rejection of all four null hypotheses. Governance Policies and Roles recorded the strongest correlation (r = 0.735), which is explained by the fact that written policies and defined accountability structures are the most visible and directly experienced governance mechanisms from an employee perspective, as they shape daily behavior, set expectations, and carry disciplinary consequences, making their perceived impact on protection outcomes the most immediate and tangible. Data Lifecycle Management (r = 0.707) and Access Control and Security (r = 0.690) both demonstrated strong relationships, reflecting the operational centrality of these dimensions in daily practice, since employees interact with access control procedures and data handling protocols on a routine basis, making their connection to protection outcomes perceptually clear and consistent. Data Quality Management recorded the weakest correlation (r = 0.563), which is analytically explained by the complete absence of data quality policies identified in the documentary analysis. Without a formal policy framework anchoring data quality as a governance obligation, employees practice it as an operational necessity rather than a conscious protection mechanism, weakening its perceived direct link to personal data protection. The multiple

regression further revealed that when all four sub-dimensions are considered simultaneously, Data Quality Management loses statistical significance ($p = .230$), confirming that its contribution to personal data protection is largely mediated through its overlap with the other three dimensions rather than operating as an independent protective mechanism, a finding consistent with the theoretical position that data quality is a prerequisite condition enabling other governance functions rather than a standalone protection instrument.

3. Comparison with Literature

The findings of this study largely confirm the theoretical positions advanced in the literature while offering empirical specificity that existing studies have not provided in the Algerian private sector context.

The characterization of Condor Electronics as operating at a low level of data governance maturity is consistent with the broader pattern identified across the literature. Wulandari (2020) found a maturity level of 1.35 at the National Archives of Indonesia using the Stanford Data Governance Maturity Model, describing a context where continuous refinement of people, policies, and capabilities is required. The present study's findings mirror this profile: practices exist and are perceived positively by employees, but the absence of a unified framework, undefined governance roles, and the vacancy of the IT Standards and Governance Manager position since 2023 collectively place Condor Electronics at the ad hoc to initial stage of the capability maturity continuum described by Sargiotis (2024). Chukwurah et al. (2024) identified leadership support deficits, data silos, and change resistance as the primary barriers to governance framework development, all three of which are present at Condor: the removal of the governance manager role signals a leadership-level deprioritization of governance, the fragmentation of provisions across nine separate policy documents reflects a siloed approach, and employee resistance to using secure communication channels was explicitly cited by the CISO as an ongoing challenge.

The relationship between data governance and personal data protection confirmed empirically in this study is consistent with the theoretical position advanced by Julakanti et al. (2025), who argue that governance frameworks provide the structural foundation on which personal data protection is delivered through policies, roles, and access control mechanisms. The regression result ($R^2 = 0.671$, $p < .001$) provides quantitative confirmation of this argument in a private sector manufacturing context, which existing literature has not examined. The finding that Governance Policies and Roles is the strongest predictor of

personal data protection outcomes (r = 0.735) aligns with Ketmaneechairat et al. (2024), who propose that governance structures and controls must be integrated throughout the data lifecycle to effectively address personal data protection, with policy and role assignment constituting the institutional backbone of this integration. The finding also resonates with Smith (2023), who underscores that data quality management, lifecycle control, and data stewardship must be coordinated practices to guarantee reliability, a position supported by the multiple regression result showing that no single sub-dimension produces its full protective effect in isolation.

The absence of a data quality management policy identified in the documentary analysis is particularly significant when read against the literature. Koltay (2016) directly identifies data governance as the solution to data quality problems, arguing that clear decision rights, policies, and accountability structures are prerequisites for effective quality management. Hikmawati et al. (2021) similarly demonstrate that Master Data Management, a data quality-oriented governance component, requires explicit role assignments and governance mechanisms to function effectively. The complete absence of such mechanisms at the policy level at Condor Electronics represents a concrete gap between the theoretical prescriptions of the literature and the organizational reality observed in this study.

The compliance orientation of Condor's governance practices is consistent with Ferrão et al. (2021), who found that most Brazilian organizations under the LGPD prioritized awareness of legal requirements over systematic governance implementation, with only 16% having a methodology for testing data protection compliance. Condor's profile is analogous: legal compliance is embedded in the policy corpus, the ANPDP registration was completed proactively, and Law No. 18-07 is explicitly referenced across multiple policy documents, yet no unified governance framework exists to systematically monitor or enforce compliance at the organizational level. This pattern is also consistent with Elgujja et al. (2024), who found that governance structures without the force of law lack the accountability mechanisms necessary to produce consistent protection outcomes, a finding that underscores the importance of the legislative framework established by Laws No. 18-07 and No. 25-11 as the normative anchor for Condor's governance practices.

The human factor challenges identified across the interviews, specifically employee resistance to change and human error, align with the findings of Justyna & Eva (2020), who demonstrated that despite awareness, the absence of effective communication and

knowledge among employees frequently leads to inadvertent errors, and that personal data protection requires active behavioral management beyond technical controls. The strong correlation between Governance Policies and Roles and personal data protection outcomes ($r = 0.735$) further corroborates this position, as it empirically confirms that investment in policy dissemination and employee training produces the most measurable protection outcomes among all governance dimensions examined, consistent with Sargiotis (2024), who identifies employee training and awareness as a major security measure that reduces insider threats by keeping staff informed of their data protection responsibilities.

Finally, the cross-border data transfer compliance provisions identified in the Cloud Services Security Policy and the Cloud Migration Strategy Policy are directly aligned with the obligations established under Art. 44 of Law No. 18-07 and the ANPDP authorization requirement, confirming Abdelli's (2020) observation that cross-border data flows necessitate national regulatory alignment with international standards, and demonstrating that Condor has translated this legal obligation into an operational governance mechanism through its policy framework.

Conclusion of Chapter III

This chapter has presented and interpreted the empirical findings of this study through a mixed-methods approach combining qualitative and quantitative evidence. The qualitative strand established that data governance practices at Condor Electronics are operationally present and formally documented across a body of ISO 27001:2022-aligned policies, yet remain structurally fragmented in the absence of a unified governance framework, formally defined roles, and any data quality management policy. The quantitative strand confirmed that these practices exert a statistically significant and strong positive effect on personal data protection outcomes, with Governance Policies and Roles emerging as the most influential dimension and Data Quality Management as the least independently effective. Triangulation across all four data sources produced a convergent picture: data governance at Condor Electronics contributes meaningfully to personal data protection, but its contribution is graduated rather than complete, constrained by the structural and policy gaps identified throughout the analysis, findings consistent with broader patterns of low governance maturity documented in comparable contexts, while offering empirical specificity not previously available for the Algerian private sector.

GENERAL CONCLUSION

Throughout this study, a single question has guided the inquiry: how does data governance, as delivered by its practices at Condor Electronics, contribute towards personal data protection? Situated within a national context where empirical research on this subject is virtually absent and where Laws No. 18-07 and No. 25-11 have introduced binding organizational obligations that remain largely unexamined at the firm level, this question carried both academic and practical stakes. Having traversed the theoretical framework, the methodological architecture, and the full body of empirical evidence, this conclusion draws together the study's findings, derives recommendations for practice, and identifies the prospects that remain open for future research.

▪ Results

Data governance at Condor Electronics contributes meaningfully to personal data protection, but this contribution is graduated rather than complete, sustained by operational practices that exist and function in the absence of a unified governance framework.

At the qualitative level, observation confirmed the presence of data governance policies in both physical and digital form, the active use of the GLPI platform for formalized access requests and issue reporting, and recurring data protection awareness sessions for incoming employees. Documentary analysis of nine ISO 27001:2022-aligned internal policies revealed a formally documented governance corpus organized around four thematic categories: information classification and data categorization, access control and security, data lifecycle management, and legal and regulatory compliance. Access control emerged as the most institutionally developed practice, with a formal multi-step request workflow, hierarchical accountability structures, and layered technical controls documented across multiple policies, reflecting a governance architecture oriented primarily toward securing access to data rather than managing it comprehensively. Legal and regulatory compliance was the most cross-cutting theme, with explicit references to Law No. 18-07 embedded across multiple policies, indicating that the legislative framework has served as the primary normative anchor for governance development at the organizational level. Critically, no data quality management policy was identified across the entire corpus, representing the most significant structural gap in the organization's governance architecture, and confirming that data quality is practiced as an operational necessity rather than a formalized governance obligation. Interview data confirmed that governance roles are informally distributed and understood through practice rather than formally defined, that the IT Standards and Governance Manager position has been vacant since 2023, a development that signals a

leadership-level deprioritization of governance oversight, and that human error and employee resistance to secure communication channels constitute the primary behavioral challenges to effective protection, consistent with evidence from comparable organizational contexts that personal data protection requires active behavioral management beyond technical controls alone.

At the quantitative level, the regression analysis established that data governance practices explain 67.1% of the variance in personal data protection outcomes ($R^2 = 0.671$, $F = 130.300$, $p < .001$), confirming a statistically significant and strong positive effect. This result is attributable to the cumulative effect of the four governance dimensions operating together, as access control, lifecycle management, compliance practices, and policy enforcement collectively create an environment in which personal data is consistently handled, protected, and monitored. The remaining 32.9% of unexplained variance reflects factors outside the scope of the instrument, including individual attitudes, organizational culture, and leadership commitment. Pearson correlation analysis confirmed significant positive relationships between all four governance sub-dimensions and personal data protection. Governance Policies and Roles recorded the strongest association ($r = 0.735$), which is explained by the fact that written policies and defined accountability structures are the most visible and directly experienced governance mechanisms from an employee perspective, shaping daily behavior and carrying disciplinary consequences. Data Lifecycle Management ($r = 0.707$) and Access Control and Security ($r = 0.690$) both demonstrated strong relationships, reflecting the operational centrality of these dimensions in daily practice. Data Quality Management recorded the weakest correlation ($r = 0.563$), analytically explained by the complete absence of data quality policies: without a formal policy framework anchoring data quality as a governance obligation, employees do not perceive it as a direct protection mechanism. Multiple regression further revealed that Data Quality Management loses statistical significance when all sub-dimensions are examined simultaneously, confirming that its contribution operates indirectly through its overlap with the other three dimensions rather than as an independent protective mechanism. All four sub-hypotheses were supported and all null hypotheses rejected.

Triangulated across all sources, the findings establish that Condor Electronics exhibits the profile of a low governance maturity organization: practices are operationally present, formally documented, and positively perceived by employees, but they function in an ad hoc and fragmented manner rather than as part of a systematic, monitored, and accountable

governance program. The contribution of data governance practices to personal data protection is real, but it would be considerably stronger if supported by a formal, unified, and role-defined governance framework.

- **Propositions**

The following propositions are addressed to Condor Electronics and, where relevant, to policymakers and practitioners operating in similar contexts.

First, and most urgently, Condor Electronics should develop and implement a formal, unified data governance framework that consolidates its existing policies under a single coordinating structure. This framework should formally define data governance roles, specifically the data steward, data owner, and data custodian, with documented responsibilities rather than role identification by job title alone. The IT Standards and Governance Manager position, which was removed in 2023 without replacement, should be reinstated or its governance oversight function formally redistributed across existing roles with explicit accountability.

Second, a data quality management policy should be developed and integrated into the existing policy corpus. The complete absence of such a policy represents the most significant governance gap identified by this study. The policy should establish minimum standards for data accuracy, consistency, and completeness across all departments, assign quality assurance responsibilities to designated roles, and integrate with the existing GLPI platform through which data errors are currently reported on an ad hoc basis.

Third, the behavioral compliance challenges identified across all four interviews, particularly the use of informal messaging applications for sharing sensitive data, should be addressed through targeted behavioral interventions beyond general awareness sessions. These could include role-specific training on the consequences of informal data handling under Laws No. 18-07 and No. 25-11, mandatory secure communication tool adoption enforced through disciplinary mechanisms, and regular phishing and social engineering simulation exercises.

Fourth, lifecycle governance should be formalized across all divisions, not only within the IS and HR Divisions. The Legal Department's current practice of withholding data deletion pending potential judicial demands, while operationally understandable, represents a documented deviation from the data minimization requirements of Law No. 18-07. A formal inter-departmental retention schedule, developed in coordination with the Legal, HR, and IS

teams and declared to the ANPDP, would resolve this inconsistency and reduce the organization's regulatory exposure.

Finally, governance maturity should be formally and periodically assessed using a recognized framework such as DAMA-DMBOK's maturity model, enabling the organization to track progress, identify emerging gaps, and demonstrate to the ANPDP the continuous improvement of its data protection governance in alignment with its legal obligations.

- ## Study Limitations

First, the study is limited to a single case within a single sector, and its findings cannot be generalized to other Algerian enterprises or industries.

Second, the scope was confined to the IS Division on the basis of purposive sampling and access constraints, excluding divisions such as Finance, Sales, and HR which handle significant volumes of personal data. The findings therefore reflect the governance perceptions and practices of a single organizational unit rather than the organization as a whole.

Third, the quantitative strand relied on employee self-reported perceptions, introducing social desirability bias, which may have inflated the strength of the observed governance-protection relationship.

Fourth, the Cronbach's alpha for the Data Lifecycle Management sub-scale ($\alpha = 0.654$) fell below the conventional threshold of 0.70, indicating limited internal consistency for that dimension and reducing confidence in its measurement precision.

Fifth, leadership commitment and organizational culture were not examined as moderating variables, despite evidence suggesting their significance in shaping governance outcomes.

- ## Study Prospects

First, future studies should investigate the governance-protection relationship across multiple organizations, enabling comparative analysis across sectors such as banking, telecommunications, and public administration where personal data processing is particularly intensive.

Second, future research should seek organization-wide samples to capture the full heterogeneity of governance perceptions and practices across all divisions.

Third, future studies should complement perception-based instruments with objective indicators such as incident frequency rates, audit findings, or compliance assessment scores.

Fourth, future instrument development should refine the DLM items, potentially drawing on validated scales from established data governance measurement frameworks.

Fifth, future research should explicitly incorporate leadership commitment and organizational culture as moderating variables, particularly given the effect of the governance manager vacancy on governance continuity.

Sixth, with Law No. 25-11 enacted only in 2025, longitudinal research tracking governance maturity as the ANPDP extends its enforcement activities would contribute evidence currently absent from the literature on regulatory pressure and governance development.

BIBLIOGRAPHY

A. Bibliography

1. Abdelli, N. (2020). Protection des données personnelles dans la loi Algérienne. *Articles Scientifiques Et Publications*, *4*(1).
2. Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008
3. Al Khatib, I., Ahmed, N., & Ndyiaye, M. (2024). GDPR Compliance of Hospital Management Systems in the UAE. *Journal of Data Science and Intelligent Systems*. https://doi.org/10.47852/bonviewJDSIS42023640
4. Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: An analysis of the literature. *Journal of Decision Systems*, *25*(sup1), 64–75. https://doi.org/10.1080/12460125.2016.1187397
5. Ali, M. I., & Ahmad Hussain, K. (2024). Unveiling the tapestry: A comparative investigation into data-protection legislation in India and Pakistan. *SOCRATES. Rīgas Stradiņa Universitātes Juridiskās Fakultātes Elektroniskais Juridisko Zinātnisko Rakstu Žurnāls / SOCRATES. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law*, *1*(28), 1–8. https://doi.org/10.25143/socr.28.2024.1.01-08
6. Batchelder, W. S. (2024). *Data Governance Handbook: A practical approach to building trust in data* (1st ed.). Packt Publishing Limited.
7. Benamrane, S., Atoui, O., Benachi, A., & Djebaili, S. (2025). PROTECTING PERSONAL DATA IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES AND SOLUTIONS. *Lex Localis - Journal of Local Self-Government*, *23*(10), 521–534. https://doi.org/10.52152/pq017800736
8. Berisha, I. S., Kerka, E. P., & Andersons, A. (2026). Personal data protection and privacy. *European Journal of Economics, Law and Social Sciences*, *10*(1), 84–94. https://doi.org/10.2478/ejels-2026-0009
9. Bollweg, L. M. (2022). *Data Governance for Managers: The Driver of Value Stream Optimization and a Pacemaker for Digital Transformation* (1st ed). Springer Berlin / Heidelberg.
10. Chukwurah, N., Ige, A. B., Adebayo, V. I., & Eyieyien, O. G. (2024). Frameworks for effective data governance: Best practices, challenges, and implementation strategies across industries. *Computer Science & IT Research Journal*, *5*(7), 1666–1679. https://doi.org/10.51594/csitrj.v5i7.1351

11. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth edition). SAGE.
12. Cveticanin, L., Luzanin, O., & Ninkov, I. (2023). PRIVACY AND PERSONAL DATA PROTECTION IN SELF-DRIVING CAR: SUGGESTION FOR LEGAL REGULATION IN SERBIA. *Balkan Social Science Review*, *22*(22), 171–189. https://doi.org/10.46763/BSSR232222171c
13. Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms. *Journal of Practical Studies in Education*, *2*(2), 25–36. https://doi.org/10.46809/jpse.v2i2.20
14. Dhakal, K. (2022). NVivo. *Journal of the Medical Library Association*, *110*(2). https://doi.org/10.5195/jmla.2022.1271
15. Dutta, H. (2016). Graph Based Data Governance Model for Real Time Data Ingestion. *International Journal of Information Technology and Computer Science*, *8*(10), 56–62. https://doi.org/10.5815/ijitcs.2016.10.07
16. DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd edition). Technics Publications.
17. Elgujja, A. A., Arimoro, A., Alshahrani, F. S., Hersi, A. S., Elgujja, A. A., & Ezreqat, S. (2024). Mobile apps for health surveillance: Balancing public health needs with the privacy of personal data. *Journal of Infrastructure Policy and Development*, *8*(11), 5703. https://doi.org/10.24294/jipd.v8i11.5703
18. Ellis, P. (2024). Research methods: Qualitative observation. *Wounds UK*, *20*(1).
19. Eryurek, E., Gilad, U., Lakshmanan, V., Kibunguchy, A., & Ashdown, J. (2021). *Data governance: The definitive guide: people, processes, and tools to operationalize data trustworthiness* (First edition). O'Reilly Media, Inc.
20. Ferrão, S. É. R., Carvalho, A. P., Canedo, E. D., Mota, A. P. B., Costa, P. H. T., & Cerqueira, A. J. (2021). Diagnostic of Data Processing by Brazilian Organizations—A Low Compliance Issue. *Information*, *12*(4), 168. https://doi.org/10.3390/info12040168
21. Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th edition). Sage.
22. Ghanad, A. (2023). An Overview of Quantitative Research Methods. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS*, *06*(08). https://doi.org/10.47191/ijmra/v6-i8-52
23. Griffiths, K. E., Blain, J., Vajdic, C. M., & Jorm, L. (2021). Indigenous and Tribal Peoples Data Governance in Health Research: A Systematic Review. *International*

Journal of Environmental Research and Public Health, *18*(19), 10318. https://doi.org/10.3390/ijerph181910318

24. Gupta, U. G. (with Cannon, S.). (2020). *A Practitioner's Guide to Data Governance: A Case-Based Approach*. Emerald Publishing Limited.
25. Gupta, U. G., & Cannon, S. (2020). A Review of Data Governance Definitions and Emerging Perspectives: *International Journal of Data Analytics*, *1*(2), 30–47. https://doi.org/10.4018/IJDA.2020070103
26. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (Eighth edition). Cengage.
27. Hikmawati, S., Santosa, P. I., & Hidayah, I. (2021). Improving Data Quality and Data Governance Using Master Data Management: A Review. *IJITEE (International Journal of Information Technology and Electrical Engineering)*, *5*(3), 90. https://doi.org/10.22146/ijitee.66307
28. Hilmy Rizqullah Ramadhan, M., Ramadhani, K., Isrok, M., Anggraeny, I., & Prasetyo, R. (2024). Legal Protection of Personal Data in Artificial Intelligence for Legal Protection Viewed From Legal Certainty Aspect. *KnE Social Sciences*. https://doi.org/10.18502/kss.v8i21.14710
29. Huff, A. S. (Ed.). (1990). *Mapping strategic thought*. Wiley.
30. Imad, C. (2024). The Protection of Personal Data in Algeria: Between Local Challenges and International Standards. *Pakistan Journal of Life and Social Sciences (PJLSS)*, *22*(2). https://doi.org/10.57239/PJLSS-2024-22.2.001329
31. Julakanti, S. R., KiranmayeeSattiraju, N. S., & Julakanti, R. (2025). *Data Protection through Governance Frameworks*. https://doi.org/10.48550/ARXIV.2502.10404
32. Justyna, Ż., & Eva, N. (2020). Personal Data Protection as an Element of Competitive Advantage. *System Safety: Human - Technical Facility - Environment*, *2*(1), 55–61. https://doi.org/10.2478/czoto-2020-0008
33. Ketmaneechairat, H., Maliyaem, M., & Puttawattanakul, P. (2024). Towards a Management System Framework for the Integration of Personal Data Protection and Data Governance: A Case Study of Thai Laws and Practices. *International Journal of Technology*, *15*(1), 219. https://doi.org/10.14716/ijtech.v15i1.5885
34. Koltay, T. (2016). Data governance, data literacy and the management of data quality. *IFLA Journal*, *42*(4), 303–312. https://doi.org/10.1177/0340035216672238

35. Krejcie, R. V., & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, *30*(3), 607–610. https://doi.org/10.1177/001316447003000308
36. Loi N° 18-07 Du 25 Ramadhan 1439 Correspondant Au 10 Juin 2018 Relative à La Protection Des Personnes Physiques Dans Le Traitement Des Données à Caractère Personnel, N° 34 Journal Officiel de la République Algérienne Démocratique et Populaire (2018).
37. Loi N° 25-11 Du 28 Moharram 1447 Correspondant Au 24 Juillet 2025 Modifiant et Complétant La Loi N° 18-07 Du 25 Ramadhan 1439 Correspondant Au 10 Juin 2018 Relative à La Protection Des Personnes Physiques Dans Le Traitement Des Données à Caractère Personnel, N° 48 Journal Officiel de la République Algérienne Démocratique et Populaire (2025).
38. Lonzetta, A., & Hayajneh, T. (2018). Challenges of Complying with Data Protection and Privacy Regulations. *ICST Transactions on Scalable Information Systems*, 166352. https://doi.org/10.4108/eai.26-5-2020.166352
39. MAFFEO, L. (2023). *DESIGNING DATA GOVERNANCE FROM THE GROUND UP: Six steps to build a data-driven culture*. O'REILLY MEDIA.
40. Mahanti, R. (2021a). *Data governance and data management: Contextualizing data governance drivers, technologies, and tools*. Springer.
41. Mahanti, R. (2021b). *Data governance success: Growing and sustaining data governance*. Springer.
42. Makwana, D., Engineer, P., Dabhi, A., & Chudasama, H. (2023). Sampling Methods in Research: A Review. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, *7*(3).
43. Masinde, J., Mugambi, F., & Muthee, D. W. (2025). Big data and personal information privacy in developing countries: Insights from Kenya. *Frontiers in Big Data*, *8*, 1532362. https://doi.org/10.3389/fdata.2025.1532362
44. Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *Vol 1*. https://doi.org/10.17169/FQS-1.2.1089
45. McDowall, R. D. (2019). *Data integrity and data governance: Practical implementation in regulated laboratories*. Royal Society of Chemistry.
46. Mishra, A. (2024). Privacy-Preserving Data Sharing Platform. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *08*(04), 1–5. https://doi.org/10.55041/IJSREM32225

47. Morgan, D. L. (2014). Pragmatism as a Paradigm for Social Research. *Qualitative Inquiry*, *20*(8), 1045–1053. https://doi.org/10.1177/1077800413513733
48. Morgan, H. (2022). Conducting a Qualitative Document Analysis. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2022.5044
49. Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, *22*, 16094069231205789. https://doi.org/10.1177/16094069231205789
50. Nunnally, J. C. (1978). *Psychometric Theory* (2nd ed.). McGraw-Hill.
51. O'brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. *Quality & Quantity*, *41*(5), 673–690. https://doi.org/10.1007/s11135-006-9018-6
52. Petrella, A. (2020). *What Is Data Governance? Understanding the Business Impact*. O'Reilly Media, Inc.
53. Pin, C. (2023). Semi-structured Interviews. *LIEPP METHODS BRIEF N°4*.
54. Plachkinova, M., & Knapp, K. (2023). Least Privilege across People, Process, and Technology: Endpoint Security Framework. *Journal of Computer Information Systems*, *63*(5), 1153–1165. https://doi.org/10.1080/08874417.2022.2128937
55. Ranganathan, P., & Caduff, C. (2023). Designing and validating a research questionnaire—Part 1. *Perspectives in Clinical Research*, *14*(3), 152–155. https://doi.org/10.4103/picr.picr_140_23
56. Roberts, R. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2020.4640
57. Saraswati, P., & Devi, A. (2023). Mixed Methods-Research Methodology an Overview. *Nursing and Health Care*, *5*(4). https://doi.org/10.30654/MJNH.100024
58. Sargiotis, D. (2024). *Data Governance: A Guide* (1st ed). Springer.
59. Shah, S. I. H., Peristeras, V., & Magnisalis, I. (2021). DaLiF: A data lifecycle framework for data-driven governments. *Journal of Big Data*, *8*(1), 89. https://doi.org/10.1186/s40537-021-00481-3
60. Smith, J. (2023). *Data Governance Strategies for Maintaining Data Integrity*. https://doi.org/10.5281/ZENODO.8415852
61. Spalević, Ž., & Vićentijević, K. (2022). GDPR and challenges of personal data protection. *The European Journal of Applied Economics*, *19*(1), 55–65. https://doi.org/10.5937/EJAE19-36596

62. Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed). Pearson Education.
63. Ugwu, C., & Eze Val, H. U. (2023). Qualitative Research. *IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES*, *8*(1).
64. Williamson, S. M., & Prybutok, V. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Applied Sciences*, *14*(2), 675. https://doi.org/10.3390/app14020675
65. Wulandari, S. A. (2020). Data Governance Maturity Level at the National Archives of the Republic of Indonesia. *Jurnal Penelitian Pos Dan Informatika*, *10*(1), 27–40. https://doi.org/10.17933/jppi.v10i1.306
66. Zanke, P., & Sontakke, D. (2024). Safeguarding Patient Confidentiality in Telemedicine: A Systematic Review of Privacy and Security Risks, and Best Practices for Data Protection. *International Journal of Current Science Research and Review*, *07*(06). https://doi.org/10.47191/ijcsrr/V7-i6-42
67. Zhuang, L. (2024). The Development and Challenges of Data Protection Laws. *International Law Research*, *13*(1), 38. https://doi.org/10.5539/ilr.v13n1p38

B. Webography

1. Bougnague, S. (2025, June 6). *What Is a Data Custodian?* Cloudficient. https://www.cloudficient.com/blog/what-is-a-data-custodian
2. Cambridge University Press. (n.d.). *Data protection*. Cambridge Dictionary. Retrieved March 12, 2026, from https://dictionary.cambridge.org/dictionary/english/data-protection
3. Condor. (2025, January 23). *Notre Historique—Condor*. https://condor.dz/notre-historique/
4. DataGuard. (n.d.). *Data protection (definition)*. Retrieved March 12, 2026, from https://www.dataguard.com/glossary/data-protection-definition
5. EDPB. (n.d.). *Data Protection Officer*. European Data Protection Board: EDPB. Retrieved March 9, 2026, from https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en
6. Gomstyn, A., & Jonker, A. (2025, May 15). *What Is Data Quality Management?* https://www.ibm.com/think/topics/data-quality-management
7. Hyseni, V. (2024, April 30). Data Protection Challenges. *PECB*. https://pecb.com/en/article/data-protection-challenges

8. IBM. (n.d.). *IBM SPSS Statistics*. IBM. Retrieved March 31, 2026, from https://www.ibm.com/products/spss-statistics
9. IBM. (2021, November 12). *Data lifecycle management*. IBM. https://www.ibm.com/think/topics/data-lifecycle-management
10. IBM. (2024, April 5). *What is Data Protection?* IBM. https://www.ibm.com/think/topics/data-protection
11. Matthew Kosinski, & Jim Holdsworth. (2024, September 20). *What is Data Governance?* https://www.ibm.com/think/topics/data-governance
12. Microsoft. (n.d.-a). *What is Data Governance?* Microsoft. Retrieved March 9, 2026, from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-data-governance
13. Microsoft. (n.d.-b). *What Is Data Protection?* Microsoft. Retrieved March 12, 2026, from https://www.microsoft.com/en-us/security/business/security-101/what-is-data-protection
14. MuleSoft. (n.d.). *What is a Single Source of Truth (SSOT)*. MuleSoft. Retrieved March 12, 2026, from https://www.mulesoft.com/resources/esb/what-is-single-source-of-truth-ssot
15. Oxford University Press. (n.d.). *data protection noun—Definition, pictures, pronunciation and usage notes*. Oxford Learner's Dictionaries. Retrieved March 12, 2026, from https://www.oxfordlearnersdictionaries.com/definition/american_english/data-protection
16. SAP. (2025, March 10). *What is data quality?* SAP. https://www.sap.com/resources/what-is-data-quality
17. Vaideeswaran, N. (2023, December 14). *Data Protection vs Data Security*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-protection-vs-data-security/

APPENDICES

Appendix A — Interview Guide

Introduction

This interview is part of research dissertation investigating how data governance practices at Condor Electronics relate to the protection of personal data. Your answers will remain strictly confidential and used for academic purposes only. There are no right or wrong answers, your honest experience is what matters.

Part I — Interviewee Profile

Q1: Could you briefly tell me about your role at Condor and the kind of data you work with on a daily basis?

Part II — Data Governance Practices

Q2: How is personal data about customers or employees maintained in terms of accuracy, completeness, and structure? For instance, if data is wrong, outdated, duplicated, or inconsistently formatted, who identifies these issues and how are they corrected?

Q3: In your department, who takes care of different parts of personal data, such as making sure it's accurate and complete, deciding who can see it, keeping it secure, managing the systems where it's stored, or giving advice about following data protection rules?

Q4: Can you walk me through what happens to personal data from the moment it is collected until it is no longer needed, is there a defined process for storing, archiving, or deleting it?

Q5: How does Condor control access to personal data, and what measures are in place to prevent unauthorized access, loss, or misuse?

Q6: To what extent are the organization's formal data-handling policies implemented, and how well are employees informed or trained about them?

Part III — Personal Data Protection

Q7: In your own experience, what do you understand by 'personal data', and where did you acquire that knowledge in the context of your role at Condor?

Q8: How do you ensure that the personal data you handle is managed according to company rules or legal requirements, and are there any challenges in following these procedures?

Q9: If a situation occurs where personal data is accessed, shared, or lost without proper authorization, even accidentally, how would your organization handle it?

Q10: In your opinion, how do the current practices in your organization (such as how data is handled, secured, and managed) help in protecting personal data?

Part IV — Closing

Thank you for your time and cooperation. Your input is invaluable to this research. As a reminder, all responses are strictly confidential, no names or identifying details will appear in the final thesis.

Appendix B — Questionnaire

Dear employee,

This questionnaire forms part of a Master's dissertation in E-Governance at the École Nationale Supérieure du Management (ENSM). It aims to examine how data governance practices contribute to the protection of personal data within Condor Electronics. Your responses will remain strictly confidential and will be used solely for academic purposes. There are no right or wrong answers, your honest reflection of your daily work experience is all that is required.

Key definitions:

Data Governance refers to the set of rules, procedures, and roles that govern how data is collected, processed, and maintained within an organization.

Personal Data refers to any information relating to an identified or identifiable natural person, such as a name, phone number, photograph, national identity number, or similar identifiers.

Section 1. Respondent Profile

Please tick (X) the appropriate box for each field.

Field	Response
Gender	Male □ Female □
Age	Under 25 □ 25–34 □ 35–44 □ 45 or above □
Educational Level	Technician Supérieur □ Licence □ Master / Engineer □
Years of Experience	Less than 1 year □ 1–3 years □ 4–7 years □ More than 7 years □

Note: For each statement in the sections below, please place a mark (X) in the box that best reflects your level of agreement, based on your actual experience at work.

Section 2. Data Quality

Data quality refers to ensuring that the information used in day-to-day work is accurate, complete, and up to date, free of errors and duplication.

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	The accuracy and correctness of data stored in my department's systems is regularly verified.					
2	There is a clear procedure in my department for correcting erroneous or duplicated data as soon as it is identified.					
3	The data I use in my work is up to date and fit for the purpose for which it was intended.					
4	Employees in my department follow a standardized format when entering data into systems (e.g., names, dates).					

Section 3. Access Control and Data Security

This refers to the systems and rules in place within the organization that prevent any unauthorized person from accessing or disclosing personal data.

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	Only employees who require it to perform their duties are able to access organizational data.					
2	There are clear procedures within my department to prevent unauthorized access to organizational data.					
3	The systems and applications used in my department protect data from loss or disclosure.					
4	Access rights to data are reviewed and updated when employees change roles or leave the organization.					

Section 4. Data Lifecycle Management

This refers to how data is handled from the moment it is received (collection), through its storage, to its archiving or secure deletion when it is no longer needed.

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	New data received by my department is reviewed before being entered into the systems.					
2	Data in my department is stored in the designated systems, not in ad hoc locations.					
3	Data that is no longer used daily in my department is not immediately deleted, but is retained in an archive for future reference when needed.					
4	Data that my department no longer requires is deleted or disposed of securely and in accordance with a defined procedure.					

Section 5. Policies and Defined Roles

This refers to whether the organization has written rules explaining how data should be handled, and whether a designated person or body is responsible for enforcing those rules.

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	Written internal regulations and policies exist within this organization that define how data is to be handled.					
2	There is a designated person or body responsible for overseeing compliance with personal data protection policies.					
3	Employee compliance with data handling rules is subject to periodic review through audits or assessments.					
4	The approved data handling procedures and policies within my department are effectively applied in daily work.					

Section 6. Personal Data Protection

This refers to safeguarding individuals' information (such as name, phone number, photograph, and address) so that it is not accessed by unauthorized persons, misused, or lost or destroyed, in a secure and lawful manner.

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	The personal data of individuals stored in my organization’s systems accurately reflects their actual information.					
2	When I identify an error in an individual's personal data, I know the correct procedure for requesting its correction.					
3	The accuracy of personal data in my organization’s systems is subject to regular monitoring.					
4	I am confident that the personal data stored in my organization’s systems is protected from unauthorized access or disclosure.					
5	The systems I use prevent me from accessing personal data that falls outside the scope of my professional duties.					
6	I am aware of my personal responsibility to maintain the confidentiality of the personal data I handle in my daily work.					

7	My department limits the collection of personal data strictly to what is necessary for the completion of each task, without collecting surplus data.					
8	Personal data is not retained beyond what is necessary for the purpose for which it was collected.					
9	I am aware that individuals have the right to request the deletion of their personal data, and that my department has a procedure for handling such requests.					
10	My department generally does not collect personal data beyond what is actually required for operational needs.					
11	I am familiar with the internal regulations and procedures governing the handling of personal data in my organization.					
12	I consistently apply personal data protection policies in my daily work.					
13	I have received adequate training or guidance on my obligations regarding the protection of personal data relevant to my duties.					
14	I feel sufficiently competent to handle personal data in a manner that respects individuals' rights.					

Experts Validation Panel

N°	Name	Title	Institution
01	Omar KADI	Doctor	ENSM
02	Islam Lebcir	Doctor	ENSM
03	Djalel YAHIAOUI	Doctor	ENSM

Appendix C — Internal Company Documents

Data Retention Declaration Document

	Catégorie	نوع المعلومات المتلقاة Types d'informations recueillies	المصدر الأصلي للمعلومة Origine de la donnée	تستعمل لغاية المعالجة Utilisé (e) pour la finalité du traitement	مصدر المعلومة Sources de données	مدة حفظ المعلومة بعد انجاز الغاية أو نهاية النشاط Durée de conservation après la réalisation de la finalité ou à la fin du contrat
9	Données à caractère personnel	Adresse du domicile	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire (●) Dossiers papiers ( ) Base de données ( ) Autre :	384 Mois
10	Données à caractère personnel	Photo	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire (●) Dossiers papiers ( ) Base de données ( ) Autre :	384 Mois
11	Données à caractère personnel	N° de téléphone	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	(●) Formulaire ( ) Dossiers papiers ( ) Base de données ( ) Autre :	384 Mois
12	Données à caractère personnel	Autre à préciser Salaire ..... الراتب	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire ( ) Dossiers papiers (●) Base de données ( ) Autre :	384 Mois
13	Données à caractère personnel	Adresse Mail	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire (●) Dossiers papiers ( ) Base de données ( ) Autre :	384 Mois
14	Données à caractère personnel	Autre à préciser Adresse Professional .... البريد الإلكتروني المهني	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire ( ) Dossiers papiers (●) Base de données ( ) Autre :	384 Mois
15	Données à caractère personnel	Situation de famille	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire (●) Dossiers papiers ( ) Base de données ( ) Autre :	384 Mois
16	Données à caractère personnel	Autre à préciser Personne référence .... الأشخاص المرجعين	(●) De la personne concernée ( ) Autre :	(●) Oui ( ) Non	( ) Formulaire (●) Dossiers papiers ( ) Base de données ( ) Autre :	384 Mois

Compliance Policy

Condor	SPA CONDOR ELECTRONICS	Code : PL.SI.13
		Date: 23/03/2025
	Politique de Conformité	Version : 03 | Public : C0
		Page : 1/6

Version : 03	Rédacteur	Vérificateur	Approbateur
Nom /Prénom	MATOUG Elyes	BELLALA Abdeslam	BOULAFRAKH Hocine
Fonction	Responsable Sécurité SI	Directeur QHSE	Directeur SI
Date	23/03/2025	23/03/2025	23/03/2025
Visa	Condor MATOUG Elyes Responsable de la Sécurité S.I. Direction des Systèmes d'Information	Condor BELLALA Abdeslam Directeur QHSE	

Les destinataires : Direction SI, Direction Générale, Direction QHSE, Structure juridique

Date d'application : Date d'approbation

ETAT DES EVOLUTIONS

N°	Nature de la modification	Version	Date de modification
01	Création	01	02/02/2021
02	Mise à jour de contenu	02	06/02/2022
03	Mise à jour de contenu selon la norme ISO 27001/2022	03	23/03/2025

SOMMAIRE

Information Security Policy

CONDOR ELECTRONICS
SPA au capital social de 4 277 000 000. 00 DA
Conception, Fabrication et Commercialisation des réfrigérateurs, congélateurs, climatiseurs, radiateurs à gaz, machines à laver lave-vaisselle, cuisinières et petits appareils ménagers.

ISO 9001:2015
ISO 14001:2015
ISO 45001:2018
Management System
www.tuv.com
ID 9105081367

Politique de la Sécurité de l'Information

À l'ère du numérique et dans un contexte concurrentiel mondialisé, l'information détient une valeur économique et stratégique décisive pour la pérennité de l'entreprise. La vulnérabilité de ce patrimoine le rend fortement exposé à de nombreuses menaces qui peuvent compromettre la sécurité de nos actifs informationnels et la continuité de nos activités.

Consciente de ces défis et soucieuse à honorer ses engagements envers ses parties intéressées, Condor s'appuie sur sa direction des systèmes d'information pour piloter la mise en place d'un Système de Management de la Sécurité de l'information, basé sur l'amélioration continue et conforme à la norme ISO 27001 afin de doter l'entreprise d'un cadre fiable et adapté pour faire face à ses enjeux.

A cet effet, notre politique SMSI se décline comme suit :

- Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information ;
- Satisfaire les exigences légales et autres applicables ;
- Développer les mesures de sécurités des systèmes d'information ;
- Assurer une proactivité pour l'intégration des solutions fiables et sécurisés ;
- Garantir la protection des données à caractères personnels ;
- Faire face aux menaces et vulnérabilités de nos systèmes d'information ;
- Assurer la performance, la fiabilité et la continuité des infrastructures IT.

Cette politique témoigne de l'importance accordée par CONDOR ELECTRONICS envers la sécurité de ses informations et de son engagement à fournir toutes les ressources nécessaires pour :

- Améliorer en permanence le Système de Management de la Sécurité de l'Information ;
- Se conformer aux exigences applicables en matière de sécurité de l'information ;
- Communiquer sur l'importance de notre SMSI et s'assurer du respect de ses exigences.

Pour ce faire, nous sollicitons toutes nos parties intéressées, internes et externes à adhérer à cette politique et veiller au respect des consignes de la sécurité de l'information.

Le Directeur des SI

Condor
Hocine BOULAFRAKH
SPA - Condor Electronics
Direction Systèmes d'Information
Zone d'Activités - B.B.Arréridj
26 FEV. 2023

Le Directeur Général

SPA - Condor Electronics
Condor
Direction Générale
Zone d'Activités - Bordj-Bou-Arréridj
26 FEV. 2023
Condor
Ahmed HARROUZ
Directeur Général

Version 2.0 _ 2023 _ C0 : Public

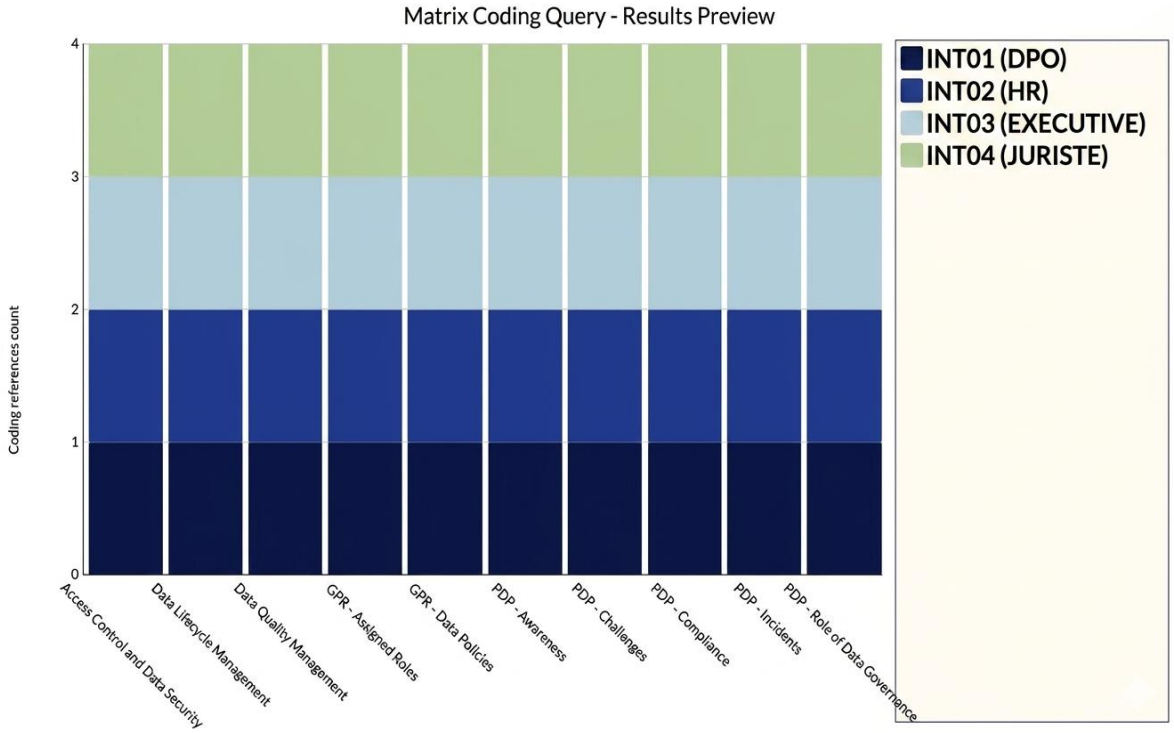
Zone d'activité Route de M'sila ilot 70, Section 161, Bordj Bou Arreridj 34000 - Algérie
Tél: +213 (0) 35 87 63 00 / +213 (0) 35 87 63 04 / Fax: +213 (0) 35 87 63 63
R.C.N°: 34/00-0462772B02 – NIS: 000234010086358 – NIF: 000234046277228
www.condor.dz / e-mail : info@condor.dz

Appendix D — NVivo Outputs

Inter-Interview Similarity Coefficients

File A	File B	Pearson correlation coefficient
Files\\IS Engineer	Files\\Data Protection Officer	0.89753
Files\\HR Officer	Files\\Data Protection Officer	0.890607
Files\\IS Engineer	Files\\HR Officer	0.829122
Files\\Legal Affairs Officer	Files\\HR Officer	0.755402
Files\\Legal Affairs Officer	Files\\Data Protection Officer	0.738549
Files\\Legal Affairs Officer	Files\\IS Engineer	0.721671

Coding References by Theme and Interviewee Role



Appendix E — SPSS Outputs

Cronbach's Alpha Reliability Statistics by Dimension

Dimension	Items (N)	Cronbach's α
Data Quality Management (DQM)	4	.852
Access Control and Security (ACS)	4	.901
Data Lifecycle Management (DLM)	4	.654
Governance Policies and Roles (GPR)	4	.767
Personal Data Protection (PDP)	14	.884
Overall Scale	**16**	**.909**

Item-Level Descriptive Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
DQM1	67	1	5	4.22	.982
DQM2	67	1	5	4.12	.913
DQM3	67	1	5	3.96	1.211
DQM4	67	1	5	4.16	.979
ACS1	67	1	5	4.51	.786
ACS2	67	1	5	4.52	.766
ACS3	67	1	5	4.37	.795
ACS4	67	1	5	4.43	.821
DLM1	67	1	5	4.09	.866
DLM2	67	1	5	4.45	.764
DLM3	67	1	5	3.48	1.375
DLM4	67	1	5	4.42	.742
GPR1	67	1	5	4.09	.981
GPR2	67	2	5	4.16	.863
GPR3	67	3	5	4.36	.667
GPR4	67	1	5	4.10	.800
PDP1	67	1	5	3.99	.961
PDP2	67	1	5	3.99	1.108
PDP3	67	1	5	3.88	1.008
PDP4	67	1	5	4.31	.802

PDP5	67	3	5	4.34	.708
PDP6	67	3	5	4.70	.551
PDP7	67	1	5	4.18	1.058
PDP8	67	1	5	3.91	.933
PDP9	67	1	5	3.90	1.116
PDP10	67	1	5	4.25	.804
PDP11	67	1	5	4.10	.923
PDP12	67	2	5	4.36	.711
PDP13	67	1	5	4.06	.952
PDP14	67	3	5	4.48	.636
Valid N (listwise)	67				

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.8079	4.6330	4.1748	.34578	67
Residual	-.73622	2.19206	.00000	.44572	67
Std. Predicted Value	-3.953	1.325	.000	1.000	67
Std. Residual	-1.639	4.881	.000	.992	67