الجمهورية الجزائرية الديمقراطية الشعبية
Ministry of Higher Education and Scientific Research
وزارة التعليم العالي والبحث العلمي
People's Democratic Republic of Algeria

HIGHER SCHOOL OF MANAGEMENT AND DIGITAL ECONOMY

H.S.M.D.E

المدرسة العليا للتسيير والاقتصاد الرقمي

Dissertation Submitted in Partial Fulfillment of the Requirements

for a Master's Degree

Specialty: Digital Management

THEME :

Analysis and mapping of personal data processing in the context of compliance with law 18-07 : CEVITAL SPA case study

Case : CEVITAL SPA

Presented by:

BENAIDA Meriem

Supervised by:

Oussama OULD MAAMAR

Academic year

2024-2025

الجمهورية الجزائرية الديمقراطية الشعبية
Ministry of Higher Education and Scientific Research
وزارة التعليم العالي والبحث العلمي
People's Democratic Republic of Algeria

HIGHER SCHOOL OF MANAGEMENT AND DIGITAL ECONOMY

H.S.M.D.E

المدرسة العليا للتسيير والاقتصاد الرقمي

Dissertation Submitted in Partial Fulfillment of the Requirements

for a Master's Degree

Specialty: Digital Management

THEME :

Analysis and mapping of personal data processing in the context of compliance with law 18-07 : CEVITAL SPA case study

Case : CEVITAL SPA

Presented by:

BENAIDA Meriem

Supervised by:

Oussama OULD MAAMAR

Academic year

2024-2025

Summary

Acknowledgements

First and foremost, Alhamdulillah — all praise and thanks are due to Allah for granting me the strength, perseverance, and guidance to complete this work.

I would like to express my deepest gratitude to ESGEN School and its administration for the enriching five-year academic journey. Their responsible management and commitment to student success provided us with the tools and support needed from the very beginning. My sincere thanks also go to all the professors of ESGEN for their dedication and knowledge.

I am especially grateful to my academic supervisor, Mr.OULD MAAMAR Oussama, for his continuous support, valuable guidance, and constructive feedback throughout this research.

My heartfelt appreciation goes to Cevital for the opportunity to carry out this work within their esteemed company. I would like to sincerely thank Mr.BENMESSAOUD Najib for his invaluable help and involvement in the development of this thesis, and my professional supervisor at Cevital, Mr. Zemam Zoubir, for his support and for giving me the opportunity to take my first steps into the professional world.

I am also very thankful to ANPDP (National Authority for the Protection of Personal Data) for their warm welcome and their assistance, which contributed significantly to an essential part of my thesis.

Finally, I would like to thank myself, my entire family, and everyone who supported me and contributed to the completion of this work.

Dedications

I dedicate this work to **my beloved family**, whose unwavering support has been my source of strength.

To **my dear parents**, my loving **mother** and **father**, who deserve the highest merit for this achievement and for my entire academic journey. Their unconditional support, immense generosity, and pride in me have always been a powerful source of motivation.

To my **brothers**: HAITEM , CHAHINE, HAMMAM, and AL-HARITH, and to my two **sisters**, KHADIDJA and YOUSSRA — thank you for your love, encouragement, and presence.

I warmly thank my uncle, BOUKHALFA Rabeh, for his continuous and boundless support, which greatly contributed to the success of this academic path.

This dedication also extends to **all those who have encouraged me**, believed in me, and supported me in this academic and personal journey.

List of Figures

List of Tables

List of Abbreviations

Abreviation	Signification
ANPDP	Autorité Nationale de Protection des Données à caractère Personnel
AI	Artificial Intelligence (Intelligence Artificielle)
CNIL	Commission Nationale de l'Informatique et des Libertés (France)
CCPA	California Consumer Privacy Act
DPO	Data Protection Officer (Délégué à la protection des données)
DPIA	Data Protection Impact Assessment (Analyse d'impact relative à la protection des données)
DPaaS	Data Protection as a Service
GDPR	General Data Protection Regulation (Règlement Général sur la Protection des Données – RGPD)
ISO/IEC 27701	International Standard for Privacy Information Management
PII	Personally Identifiable Information (Informations personnelles identifiables)
PbD	Privacy by Design (Protection de la vie privée dès la conception)
PIMS	Privacy Information Management System
RoPA	Records of Processing Activities (Registre des activités de traitement)
EU	European Union (Union européenne)
BtoB / B2B	Business to Business
BtoC / B2C	Business to Consumer
CRM	Customer Relationship Management (Gestion de la relation client)
ICT	Information and Communication Technologies (Technologies de l'information et de la communication)
KPI	Key Performance Indicator (Indicateur clé de performance)
NTIC	Nouvelles Technologies de l'Information et de la Communication
PME	Petite et Moyenne Entreprise
PIM	Product Information Management (Gestion de l'information produit)
ROPO	Research Online, Purchase Offline
ROI	Return On Investment (Retour sur investissement)

SEA	Search Engine Advertising (Publicité sur les moteurs de recherche)
SEO	Search Engine Optimization (Optimisation pour les moteurs de recherche)
SMO	Social Media Optimization
TIC	Technologies de l'Information et de la Communication
UX	User Experience (Expérience utilisateur)
E-commerce	Electronic Commerce (Commerce électronique)
ERP	Enterprise Resource Planning (Progiciel de gestion intégré)
Abréviation	Signification complète
ANPDP	Autorité Nationale de Protection des Données à caractère Personnel
ISO	International Organization for Standardization
PIA	Privacy Impact Assessment
IT	Information Technology (Technologies de l'Information)
CEO	Chief Executive Officer (Directeur Général)
QHSE	Qualité, Hygiène, Sécurité, Environnement
DSI	Direction des Systèmes d'Information
DRH	Direction des Ressources Humaines
HR	Human Resources (Ressources Humaines)
ID	Identifier (Identifiant)
CNAS	Caisse Nationale des Assurances Sociales
CASNOS	Caisse Nationale de Sécurité Sociale des Non-Salariés

Abstract

In a context where digital transformation is accelerating across Algerian enterprises, ensuring the protection of personal data has become a legal and strategic necessity. This thesis investigates how Algerian companies, specifically Cevital, can comply with Law No. 18-07 on the protection of personal data. In the context of increasing digitalization and regulatory complexity, the study addresses the need for structured data governance to ensure legal compliance and protect individual rights. The central research problem focuses on how Cevital can operationalize compliance through effective analysis and mapping of personal data processing activities.

To answer this question, a mixed methodological approach was adopted, combining legal analysis, documentary research, semi-structured interviews with key personnel from Cevital's HR and IT departments, and direct observation of compliance practices. The study draws on national legislation and international frameworks such as the GDPR and ISO/IEC 27701 to benchmark best practices.

The findings reveal that while Law 18-07 provides a solid legal foundation, its effective implementation requires significant organizational efforts, including awareness campaigns, internal documentation, and the development of a privacy governance model. Cevital has begun to integrate these elements through a compliance initiative focused on risk mapping and stakeholder engagement.

This research contributes both academically and practically by providing a framework for Algerian companies seeking to align with modern data protection standards. It highlights the strategic importance of personal data governance and the operational challenges of implementing regulatory compliance in the digital age.

Résumé

Dans un contexte marqué par la montée en puissance du numérique en Algérie, la protection des données personnelles s'impose comme un enjeu juridique et stratégique incontournable.

Ce mémoire examine comment les entreprises algériennes, en particulier Cevital, peuvent se conformer à la Loi n°18-07 relative à la protection des données à caractère personnel. Dans un contexte marqué par la transformation numérique et la montée des exigences réglementaires, l'étude s'interroge sur la nécessité d'une gouvernance structurée des données afin d'assurer la conformité juridique et de protéger les droits des individus.

Pour y répondre, une méthodologie mixte a été adoptée : analyse juridique, recherche documentaire, entretiens semi-directifs avec les départements RH et IT de Cevital, et observation directe des pratiques internes. Le cadre légal algérien a été comparé aux normes internationales telles que le RGPD et l'ISO/IEC 27701.

Les résultats montrent que, bien que la Loi 18-07 constitue un socle juridique solide, son application efficace requiert des efforts organisationnels importants, notamment en matière de sensibilisation, de documentation interne, et de mise en place d'une gouvernance de la vie privée. Cevital a entamé un processus de mise en conformité basé sur la cartographie des risques et l'engagement des parties prenantes.

Cette recherche apporte une double contribution : académique, en enrichissant le champ de la gouvernance des données, et pratique, en proposant un cadre de référence aux entreprises algériennes souhaitant se conformer aux standards modernes de protection des données.

ملخص

في ظل التحول الرقمي المتسارع الذي تشهده المؤسسات الجزائرية، أصبحت حماية البيانات الشخصية ضرورة قانونية واستراتيجية ملحة.

تتناول هذه المذكرة كيفية امتثال الشركات الجزائرية، وعلى رأسها شركة سيفيتال، لأحكام القانون رقم 18-07 المتعلق بحماية البيانات ذات الطابع الشخصي. في ظل التعقيد التنظيمي المتزايد، تسلط الدراسة الضوء على أهمية حوكمة البيانات المهيكلة لضمان الامتثال القانوني وحماية حقوق الأفراد.

وللإجابة على إشكالية البحث، تم اعتماد منهجية متعددة الأساليب شملت: التحليل القانوني، البحث الوثائقي، مقابلات شبه موجهة مع مسؤولي الموارد البشرية وتكنولوجيا المعلومات في سيفيتال، والملاحظة المباشرة لممارسات الامتثال. واستندت الدراسة إلى التشريعات الوطنية والمعايير الدولية مثل اللائحة العامة لحماية البيانات (GDPR) والمعيار ISO/IEC 27701 كنماذج مرجعية.

وقد أظهرت النتائج أن تطبيق القانون 18-07 يتطلب جهوداً تنظيمية كبيرة، تشمل حملات توعوية، توثيقاً داخلياً، وتطوير نموذج لحوكمة الخصوصية. وقد بدأت سيفيتال فعلياً في دمج هذه العناصر من خلال مبادرة امتثال تعتمد على تحليل المخاطر وإشراك الأطراف المعنية.

وتسهم هذه الدراسة في إثراء الجانب الأكاديمي وفي تقديم حلول عملية للشركات الجزائرية التي تسعى لمواءمة عملياتها مع المعايير الحديثة لحماية البيانات في العصر الرقمي.

Introduction

In today’s interconnected world, digital technologies have profoundly transformed the way individuals, organizations, and states operate. The rise of the digital economy, the proliferation of connected devices, and the mass adoption of cloud computing, artificial intelligence (AI), and big data have created an environment where information circulates continuously and instantaneously. In this new digital paradigm, data has become a central strategic resource — the "new oil" of the 21st century — enabling decision-making, innovation, economic value creation, and public policy design.

Within this data-driven ecosystem, personal data occupies a particular place due to its inherent connection to human identity, privacy, and dignity. Unlike industrial or financial data, personal data — such as names, biometric identifiers, health records, and geolocation — is directly linked to individuals and reflects their physical, physiological, social, or behavioral traits. The collection, storage, use, or sharing of such data is no longer a purely technical act; it raises essential legal, ethical, and societal questions.

The processing of personal data, particularly when carried out on a large scale or for sensitive purposes (surveillance, profiling, behavioral targeting), presents significant risks to fundamental rights and freedoms. Issues such as unauthorized access, discrimination, surveillance capitalism, and algorithmic bias have placed data protection at the heart of global regulatory debates. In response, many countries have adopted specific legal frameworks aimed at guaranteeing the responsible and lawful use of personal data.

Among the most influential regulatory instruments is the General Data Protection Regulation (GDPR), implemented in the European Union in 2018, which has become a global benchmark for personal data governance. The GDPR establishes core principles such as lawfulness, transparency, purpose limitation, data minimization, and accountability, and introduces new rights for individuals (e.g., right to be forgotten, data portability). It also emphasizes the importance of compliance tools, such as the Register of Processing Activities, Data Protection Impact Assessments (PIAs), Data Protection Officers (DPOs), and privacy by design. Alongside the GDPR, international standards such as ISO/IEC 27701 (Privacy Information Management System), OECD Guidelines on the Protection of Privacy, and the

Council of Europe Convention 108+ have contributed to harmonizing best practices across jurisdictions.

Faced with these global developments and in recognition of the strategic importance of protecting its citizens' data, Algeria adopted Law No. 18-07, enacted on June 10, 2018, concerning the protection of individuals in the processing of personal data. This law represents a major step forward in aligning the national legal system with international standards, by defining personal data, establishing legal bases for processing, creating an independent regulatory authority (ANPDP), and setting out obligations for public and private actors.

However, the adoption of a law alone is not sufficient. The real challenge lies in its effective implementation, and more specifically, in the capacity of organizations to ensure compliance. Compliance entails not only legal knowledge but also organizational readiness, internal documentation, staff training, risk management, and continuous interaction with the regulatory authority. It is a complex, multidisciplinary process that requires coordination between legal, technical, and managerial domains.

It is precisely this issue — the operationalization of compliance with Law 18-07 in Algerian enterprises — that constitutes the central theme of this research.

Given the context outlined above, and considering the growing legal and operational complexity of personal data protection in Algeria, the issue of effective compliance becomes central. In particular, large organizations like Cevital face the dual challenge of understanding the legal expectations of Law 18-07 and translating them into operational and traceable internal mechanisms.

From this observation arises the following central research problem:

How can Cevital achieve compliance with the legal requirements of Law 18-07 on the protection of personal data, through a structured approach to analysis and mapping of data processing operations?

This question requires a multidisciplinary perspective, combining legal interpretation with organizational and technical analysis.

To explore this problem in depth, the following sub-questions have been defined:

1. What are the legal and operational requirements of Law 18-07 concerning the compliance of personal data processing operations, and how do these requirements influence the need for reliable mapping within organizations?
2. What are the internal governance structures and responsibilities within Cevital related to personal data protection, and how are these roles organized to ensure legal compliance?
3. What strategy and methodology has Cevital adopted in initiating its compliance process with Law 18-07, particularly in terms of stakeholder engagement and procedural planning?
4. What technical and procedural measures has Cevital implemented to ensure the operational success of its compliance efforts, particularly concerning the analysis and mapping of personal data processing?

- **Research Hypotheses of the Study**

To guide the legal and operational analysis conducted in this study, a series of **working hypotheses** were formulated at the outset. These hypotheses were intended to structure the research process by identifying key assumptions surrounding the interpretation and practical application of **Law 18-07** within the organizational setting of **Cevital**, a major Algerian industrial group. The aim was not to confirm preconceived notions, but to create a critical framework through which legal texts, internal processes, and institutional behaviors could be examined and assessed.

More specifically, the study advanced the following working hypotheses:

1. **On Legal Requirements and the Role of Mapping**: It was hypothesized that Law 18-07, while asserting the principles of personal data protection, does not impose detailed internal obligations such as maintaining a register of processing activities or developing a structured mapping of data flows. The assumption was that such tools might be recommended in best practices but not mandated by law.

2. **On Internal Responsibility Structures**: It was assumed that responsibility for data protection compliance is predominantly centralized within the Legal Department, with

other departments—such as Human Resources or Information Systems—playing only marginal or consultative roles in the implementation process.

3. **On the Strategic Nature of Compliance**: The study posited that compliance with Law 18-07 at Cevital would likely be approached in an ad hoc or reactive manner, driven by immediate regulatory needs rather than embedded within a broader, long-term strategic vision or formalized compliance roadmap.

4. **On the Nature and Depth of Operational Measures**: It was further hypothesized that the company's compliance efforts would primarily focus on legal documentation—such as policies and charters—and would not extend to the development of integrated digital tools, training mechanisms, or organizational instruments designed to operationalize the legal framework in daily practice.

- **Motivation for Choosing the Research Topic**

The choice of this research topic is the result of a convergence between objective academic and professional considerations and personal interest in the evolving field of digital law and data governance.

Objective Motivations

First, the topic of compliance with personal data protection regulations represents a current and strategic issue in both the legal and managerial fields. The enactment of Law 18-07 in Algeria, combined with the global momentum generated by the GDPR and international standards (ISO 27701, PIA, etc.), has placed this subject at the heart of public and private sector concerns. It is a new and underexplored topic in the Algerian academic context, which adds to its scientific relevance.

Second, this theme responds to a legal imperative: all organizations that process personal data are now required to comply with a set of obligations that are both technical and organizational. Studying this subject therefore meets a real societal and institutional need in Algeria.

Finally, the subject is perfectly aligned with my academic background in digital management. It bridges technology, law, and organizational strategy — all central components of my field of study. This allowed me to approach the topic not only from a legal point of view but also through an operational and systemic lens.

Subjective Motivations

On a more personal level, I have long been interested in data governance, the ethical dimension of digital technologies, and the role that regulatory frameworks play in protecting individuals in the digital age. The topic of personal data protection resonates with my values of responsibility, transparency, and digital citizenship. Working on this theme allowed me to deepen my understanding of the digital transformation challenges faced by Algerian organizations, while also engaging with a subject that I find intellectually stimulating and professionally relevant.

- **Research Objectives**

The present study is structured around a set of objectives designed to guide both the legal analysis and the empirical investigation carried out within the company Cevital. These objectives reflect the dual ambition of the thesis: to contribute to the academic understanding of Law 18-07 and to support its operational implementation in an organizational context.

General Objective

To analyze how Cevital can achieve compliance with the legal requirements of Law 18-07 by developing a structured approach to documenting, mapping, and managing personal data processing operations.

Specific Objectives

To achieve this overall goal, the research seeks to:

1. Clarify the legal and operational requirements of Law 18-07 in relation to data processing compliance, with a particular focus on the obligations imposed on data controllers.

2. Identify the internal governance structures and roles responsible for data protection within Cevital, and assess their involvement and coordination in the compliance process.
3. Examine the strategy, planning, and tools adopted by Cevital to launch its compliance initiative, including awareness campaigns, documentation tools, and legal inventories.
4. Evaluate the technical and procedural measures implemented by the company to ensure the traceability, security, and legality of its data processing activities — particularly through the creation of a legal mapping model.

These objectives will guide the structure of the research, the fieldwork methodology, and the analysis of results, in order to produce both academic insights and operational recommendations.

- **Importance of the Research**

This research carries a dual importance, both scientific and practical.

From an academic perspective, the study contributes to a field that remains little explored in Algeria: the operational implementation of Law 18-07 within organizations. By combining legal analysis with an applied case study, it offers a structured and contextualized understanding of data protection compliance, relevant for researchers and students in digital management and law.

From a practical standpoint, the research provides Cevital — and other Algerian companies — with actionable tools and methods to initiate and structure their compliance efforts. It also supports a broader national goal: fostering a culture of digital accountability, legal traceability, and institutional transparency in the context of Algeria's digital transformation.

- **Research Methodology and Tools**

This study adopts a descriptive, analytical, and exploratory approach, allowing both a theoretical understanding of the legal framework and a practical analysis of its implementation within an organizational context.

The methodology combines:

- Documentary research, used to study Law 18-07 and relevant international standards (GDPR, ISO 27701, etc.),
- Semi-structured interviews, conducted with key actors from the Human Resources and IT departments at Cevital, as well as exchanges with the ANPDP,
- Direct observation, which enabled the analysis of internal practices and tools during the compliance process.

This methodological triangulation ensured the reliability of the findings while offering a comprehensive view of the compliance dynamics observed in the field.

- **Plan**

To respond to the central research question concerning the implementation and compliance with Law 18-07 on the protection of personal data in Algeria, this thesis is structured into two principal parts: a theoretical framework and a practical application.

The first part, which lays the theoretical foundations, begins with a chapter entitled "Theoretical Foundations and Conceptual Framework of Personal Data Protection". This chapter defines key concepts such as personal data, data processing, consent, and privacy principles, in order to build a solid conceptual base for the study.

This is followed by a section 1 on the "Global Context, Challenges, and Personal Data Processing", which explores how data protection issues are approached globally. It highlights international trends, emerging risks, and operational challenges, especially in the digital era, providing a broader perspective for understanding the local context.

The second section , "Legal Framework and International Comparison", focuses on the normative dimension. It compares Algeria's Law 18-07 with major international frameworks, particularly the General Data Protection Regulation (GDPR) of the European Union. This comparative analysis helps identify strengths, weaknesses, and areas of alignment or divergence.

The third section , “Mapping Law 18-07: Legal Architecture of Personal Data Protection and Processing”, provides an in-depth analysis of the law’s internal structure, including rights of individuals, duties of data controllers, and mechanisms of regulation and enforcement. This legal mapping is essential for interpreting how the law is meant to function in practice.

The second part of the thesis is devoted to the practical study. It starts with “Compliance with Law 18-07: Case Study and Practical Insights”, based on a field investigation conducted within the company Cevital. The chapter “Company Overview and Data Processing Context” introduces the organizational environment and the relevance of data protection issues within it.

Then, the section “Context and Objectives of the Compliance Project” explains the motivations, methodology, and goals behind the compliance assessment carried out in the company.

The final section , “Analysis and Mapping of Processing Activities – HR Department”, presents the detailed operational analysis of how personal data is managed within the Human Resources department. It evaluates compliance with legal requirements, identifies potential gaps, and proposes corrective measures.

The thesis concludes with a general conclusion summarizing the main findings, assessing the level of alignment with Law 18-07, and offering recommendations for improved compliance and better personal data governance in Algerian organizations.

Chapter 1 : Theoretical Foundations and Conceptual Framework of Personal Data Protection

Chapter 1 : Theoretical Foundations and Conceptual Framework of Personal Data Protection

Introduction

In the context of accelerating digital transformation, the protection of personal data has emerged as a central concern for individuals, organizations, and governments worldwide. Data is no longer a simple byproduct of administrative activities—it is a strategic asset, an economic resource, and a powerful tool that can either enable innovation or threaten fundamental rights. Yet, the unprecedented volume and complexity of data processing have created new vulnerabilities and ethical dilemmas, forcing societies to rethink how data is collected, used, stored, and secured.

This chapter offers a comprehensive theoretical foundation for understanding the conceptual and legal underpinnings of personal data protection. It begins by situating data protection within its global context, identifying the societal, legal, and technological challenges posed by mass data collection and digital surveillance. It then introduces the essential terminology required to navigate this domain, including distinctions between personal data, sensitive data, anonymisation, and pseudonymisation.

The chapter also examines core data protection principles such as lawfulness, fairness, purpose limitation, and accountability—principles embedded in global standards like the General Data Protection Regulation (GDPR) and the ISO/IEC 27701 privacy framework. These are not merely abstract ideas; they form the operational criteria against which compliance, risk management, and ethical governance are evaluated.

Finally, the chapter explores the Algerian legal framework for data protection, focusing in particular on Law No. 18-07. Through comparative analysis and visual cartography, it assesses how this national law aligns with or diverges from international models. This dual approach—conceptual and legal—lays the necessary groundwork for the subsequent analytical phase of this thesis, which will evaluate the implementation and impact of these norms within real organizational settings.

Section 1 : Global Context, Challenges, and Personal Data Processing

As personal data becomes a cornerstone of the digital economy, understanding its global significance and associated challenges is essential. This section explores how evolving technologies have increased data vulnerability and the urgency of protection frameworks.

1. Historical Perspective

As the world experiences a digital transformation and technological advancement, personal data has emerged as a primary and important asset in economic and institutional transactions, and even in the systems of modern societies. From the economic aspect, which includes e-commerce, e-banking, digital investment, electronic payment systems, and others, to the field of healthcare and medical data analysis, smart cities, artificial intelligence, and digital currencies, personal data is being collected, analyzed, and transferred daily in huge quantities. This rapid development has created a strong need for the establishment of clear and robust legal foundations and frameworks to ensure respect for individuals' rights and the protection of their personal data.

The concept of personal data protection emerged as a legal principle in the early 1970s. Germany was the first to enact a national data law in 1970, followed by Sweden in 1973, and France in 1978 (Greenleaf, 2011) .These early regulations aimed to control how personal data was handled within both public institutions and private companies, especially with the growing use of computer systems. Over the following decades, data protection has evolved from a local regulatory issue to a global human rights issue.

This development was marked by a major turning point in 2016 when the European Union adopted the GDPR, which entered into force in May 2018 (Voigt, 2017). The GDPR replaced the outdated 1995 Directive, introducing a unified legal framework designed to address the challenges of the digital era, including cross-border data flows, algorithmic decision-making, and growing surveillance risks. As stated in its recitals, the GDPR seeks to protect natural persons in the digital world and reaffirms the status of personal data protection as a fundamental right under the Charter of Fundamental Rights of the European Union (European Union, 2016).

In Algeria, the legal landscape followed a similar path. In the absence of a unified legal framework dedicated to data protection, and with increasing digital risks and the need to align with international standards, the country enacted Law No. 18-07 on June 10, 2018 (République Algérienne Démocratique et Populaire, 2018). This law marked a significant shift by establishing a national legal framework that protects individuals with regard to the processing of their personal data.

This chapter addresses the theoretical foundations of personal data protection by explaining key terms, legal principles, and the regulatory aspects of data processing. It also provides the foundations for understanding how modern legal systems—most notably Law 18-07—are structured to safeguard personal data in a globally connected digital environment

2. Key Terminology and Core Concepts

Before delving into legal systems, it is necessary to clarify the key concepts surrounding personal data and its protection. This section defines the foundational terms that structure data privacy laws.

2.1 – Personal Data: Definition

The definition of personal data in the field of data protection serves as the foundation for determining the scope and applicability of legal obligations .This term refers to all information relating to individuals that allows for their identification, whether directly or indirectly. This concept is comprehensive and covers a wide range of forms, contexts, and identifiers.

Article 4 of the General Data Protection Regulation (GDPR), which is considered a global reference for privacy legislation, defines personal data as:
“ any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person ” ((European Union, 2016, pp. chapter 1, article 4 L119/33).

In the same context, Article 3 of Algerian Law 18-07, which governs the protection of personal data in Algeria, states that:
« Données à caractère personnel » : toute information, quel qu'en soit son support, concernant une personne identifiée ou identifiable, ci-dessous dénommée « personne concernée », d’une manière directe ou indirecte, notamment par référence à un numéro d’identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, biométrique, psychique, économique, culturelle ou sociale (République Algérienne Démocratique et Populaire, 2018, pp. Article 3, p11)

The translation and interpretation of this definition indicates that personal data includes any information, regardless of its form, that relates to an identified or identifiable individual

known as the data subject. This identification can occur directly or indirectly, for example through an of an identification number or specific details related to a person's physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity.

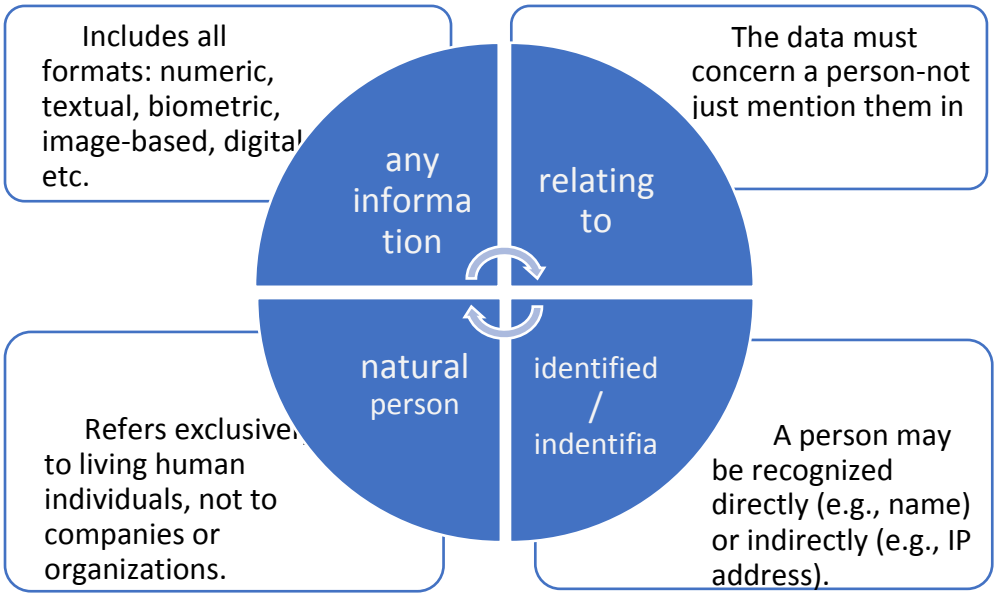
As with the European Regulation, this definition does not limit personal data to any specific type of media or form. It applies to written documents, digital records, even audio files, images, fingerprints, and any other format linked to an individual's data.
This is reflected in the experience "regardless of form or nature," which underscores the Algerian law's coverage of both paper and digital data.

An analysis of these definitions reveals significant alignment in their core components:
they all emphasize the notion of "identifiability," whether direct or indirect, and acknowledge a wide range of identifiers, such as names, ID numbers, location data, and digital identifiers. Despite minor differences in wording, these definitions share a common understanding of the broad and adaptable nature of personal data protection, encompassing any detail through which a person's identity may be inferred.

Therefore, laws governing personal data protection are built on a shared foundation in their definition of personal data. Based on this, we can conclude that a comprehensive definition includes both the notion of "identifiability" and the recognition of a wide variety of identifiers, which may appear in multiple contexts and formats.

To explore the legal scope of personal data further, Eduardo Ostaran, in his book "European Data Protection: Law and Practice," proposes a harmonized model based on 4 key elements.

Figure 1: the four 'building blocks' of the meaning of personal data



Source : Author's elaboration based on (Ustaran, 2018, p. 74)

This conceptual framework provides a clearer understanding of the legal aspects of data protection.

Accordingly, any information that can be used to identify a specific individual — regardless of whether it is stored digitally or on paper — is protected under both the GDPR and Algerian Law 18-07.

Box 1 : Example of personal data

Box 1.2 Examples of Information About Individuals Capable of Amounting to 'Personal Data'

.

Name	Shoe size	Last time/place credit card used
Address	DNA sample	Geographical location
Date of birth	Blood group	Medical history
NI number Passport number	Credit card number	Sexual preference
	Favourite restaurant	Destination of air travel

Source : (Carey, 2018, p. 14)

2.2 – Special Categories of Data: Sensitive Data

Article 9 of the GDPR, in chapter 2 under the title “Processing of special categories of personal data” defines sensitive data as a specific category of personal data that requires heightened protection. The article states :

“ Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. ” (European Union, 2016, pp. Article 9 chapter 2 , L119/38)

According to this regulation, processing of sensitive data is prohibited unless certain conditions are met, such as obtaining explicit consent or fulfilling other legal obligations.

In the same context, the relevant Article 3 of the Algerian Law defines the sensitive data as: "Données sensibles : données à caractère personnel qui révèlent l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance syndicale de la personne concernée ou qui sont relatives à sa santé, y compris ses données génétiques." (République Algérienne Démocratique et Populaire, 2018, pp. 11,Article 3)
This can be translated as:
“Sensitive data includes personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership of the data subject, or is related to their health, including genetic data.”

We can observe a strong similarity between the definitions of sensitive data provided by Algerian law and European regulation. This indicates the importance of handling this information with particular caution and applying stronger safeguards, due to its sensitive nature and the potential impact it may have on individual’s privacy .

2.3 – Data Subject : Who is Protected by Data Protection Laws ?

A data subject is, in a general sense, the person about whom any given personal data record information, or to whom the data relate.

The definition of data subject in the GDPR, which forms part of the definition of 'personal data' in Article 4(1) rather than being afforded its own defining sub- paragraph, refers to a person who is either 'identified or identifiable' :

" Data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be

(b) substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority; " (European Union, 2016, p. Article 4(1))

The concept of 'identifiability' broadens the previous definition of data subject to include individuals whose identity is not known at the time the data are col- lected but who may be identified in the future—for example, where a controller undertakes additional research or investigation, or adds additional data. (Carey, 2018, p. 11)

In Algerian Law No. 18-07, the definition of data subject is provided in Article 3, which states:
"Personne concernée : toute personne physique à l'égard de laquelle des données à caractère personnel font l'objet d'un traitement." (European Union, 2016, p. Article 3)
Translated, this means:
"Data subject: any natural person whose personal data is subject to processing."

Both Algerian lawand European regulation highlight the rights of individuals regarding their personal data, and aim to protect them from unauthorized or unlawful data processing.

2.4 – Data Controller and Data Processor: Roles and Responsibilities

Both the General Data Protection Regulation (GDPR) and Algeria's Law No. 18-07 establish clear definitions and legal obligations for two key actors in data processing: the data controller and the data processor.

Under the GDPR, the data controller is the natural or legal person who determines the purposes and means of processing personal data (European Union, 2016, p. Art. 4(7), while the processor acts on behalf of the controller and processes data according to the controller's instructions (European Union, 2016, p. Art. 4(8). These roles are reinforced by legal obligations relating to transparency, fairness, and accountability in all data operations.

Similarly, Law 18-07 defines the "responsable du traitement" as the individual or entity that determines the purposes and methods of processing, and the "sous-traitant" as the entity processing data on behalf of the controller (République Algérienne Démocratique et Populaire, 2018, pp. Art. 3, JO n°39, 2018). While the terminology differs slightly, the legal meaning aligns closely with the European framework.

Both laws impose a shared set of principles that govern the responsibilities of controllers and processors, including

- Processing must be lawful, fair, and transparent.
- Data must be collected for explicit and legitimate purposes and not further processed incompatibly.
- Only data that is relevant, adequate, and non-excessive may be processed.
- Data must be accurate and up to date.
- Retention must be limited to the time necessary for the original purpose.
- Data must be kept confidential and secure throughout the lifecycle.
- Controllers and processors must register with the national data protection authority (ANPDP).

In both legal systems, the controller bears primary responsibility for ensuring compliance, while the processor must follow instructions under a clear contractual framework. This distinction reflects the broader principle of accountability, emphasizing the need for defined

roles, proper documentation, and compliance-by-design in all personal data processing operations.

2.5 – Data Protection Officer (DPO): Function and Importance

Under the General Data Protection Regulation (GDPR), the designation of a Data Protection Officer (DPO) is mandatory in cases where personal data processing is conducted by public authorities, involves large-scale monitoring, or concerns special categories of data (European Union, 2016, p. Art. 37). The DPO acts as an independent expert, tasked with ensuring compliance, advising internal teams, conducting audits, managing risks, and serving as the liaison with supervisory authorities.

In contrast, Algeria's Law No. 18-07 does not explicitly mention the role of a DPO. However, compliance responsibilities are attributed to the data controller (responsable du traitement), and Article 10 requires organizations to adopt appropriate measures for data protection. According to expert Tadjeddine Bachir (2024), the "Focal Point" d (BACHIR, 2024)esignated by the Autorité Nationale de Protection des Données à caractère Personnel (ANPDP) plays a functionally equivalent role to that of a DPO.

The Focal Point is expected to

- Maintain a detailed register of data processing activities;
- Conduct risk assessments and implement Data Protection Impact Assessments (DPIAs) for high-risk processing;
- Ensure incident management, including breach notifications to the ANPDP (European Union, 2016, p. Art. 43);
- Promote employee awareness, monitor compliance with internal policies, and support international data transfer controls;
- Embed Data Protection by Design and by Default into organizational projects;
- Act as a contact point with the ANPDP, using formal communication channels established by the authority;
- Respond to data subject requests in line with Articles 34–36, covering rights of access, rectification, and objection;

- Apply a continuous improvement approach to adapt governance practices to legal and operational developments (BACHIR, 2024).

Although framed differently in Algerian law, the Focal Point shares the core objectives of the GDPR's DPO: to serve as a guarantor of lawful processing and as a strategic advisor supporting digital transformation. As emphasized by Bachir, this role is not merely administrative—it is central to compliance, transparency, and public trust.

2.6 – Anonymisation and Pseudonymisation: Key Differences

Under the GDPR, anonymisation and pseudonymisation are two data protection techniques used to reduce privacy risks, but they differ significantly in legal effect.

Anonymisation refers to the process of irreversibly altering personal data in such a way that the data subject can no longer be identified, directly or indirectly, even when combined with other available information. According to Recital 26 of the GDPR, once data is truly anonymised, it is no longer considered personal data and falls outside the scope of data protection obligations. This technique is commonly used for statistical or research purposes.

In contrast, pseudonymisation, as defined in Article 4(5) of the GDPR, involves replacing identifiers with a code or pseudonym while keeping a separate key that could re-identify the data subject. Because re-identification is still possible, pseudonymised data remains subject to all GDPR obligations. As Carey (2020) explains, pseudonymisation is a risk mitigation tool, not a method to remove data from the regulation's scope. It supports compliance by limiting access to direct identifiers and reducing the impact of data breaches but does not eliminate legal responsibilities.

The key distinction is that anonymisation results in non-personal data, while pseudonymisation preserves a potential link to the data subject, keeping it within the legal definition of personal data.

While Algeria's Law No. 18-07 does not explicitly define these terms, its general principles suggest alignment with the GDPR: anonymised data is likely excluded from legal obligations, whereas pseudonymised data remains regulated due to the residual identifiability it retains.

2.7 – Profiling and Automated Decision-Making: Concepts and Risks

Profiling and automated decision-making are becoming increasingly common in data processing activities, especially with the growing use of algorithms and machine learning. These concepts are designed to improve the efficiency of data analysis and decision-making but introduce several privacy and ethical concerns.

❖ Profiling :

Under the General Data Protection Regulation (GDPR), profiling is defined in Article 4(4) as:

" profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;." (European Union, 2016, p. Article 4(4))

Carey elaborates that this definition is intrinsically linked to several rights afforded to data subjects. Specifically, Articles 13(2)(f) and 14(2)(g) of the GDPR mandate that individuals be informed about the existence of profiling, the logic involved, and the significance and envisaged consequences of such processing. Moreover, Articles 21 and 22 provide individuals with the right to object to profiling in certain circumstances.

In practical applications, profiling often arises from the use of cookies on websites to analyze user preferences and behaviors. Such practices can lead to targeted advertising, credit scoring, or recruitment processes. However, the potential for bias and discrimination in these processes is substantial. Cavoukian (2013) notes that profiling can result in negative impacts on individuals, such as unjustified exclusion or unfair treatment, particularly when sensitive personal data like health or political opinions are involved (Cavoukian, 2013).

❖ Automated Decision-Making:

Automated decision-making, as outlined in Article 22 of the GDPR, refers to:

"decisions based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her." (European Union, 2016, p. Article 22)

This can lead to significant consequences, such as the denial of a loan or a job offer, without human intervention. The GDPR provides individuals with safeguards, including the right not to be subject to decisions based solely on automated processing, unless certain conditions are met, such as explicit consent or a contract necessity.

Risks and Safeguards:

Both profiling and automated decision-making raise critical concerns regarding privacy**,** fairness**,** and transparency. As Binns (2018) notes, these systems can unintentionally reinforce biases or fail to consider individual circumstances—such as in algorithmic hiring systems trained on biased datasets (Binns, 2018)

The GDPR addresses these risks by granting individuals the right not to be subject to decisions based solely on automated processing that significantly affects them. It also guarantees the right to contest such decisions and to obtain meaningful human intervention. However, enforcing these rights can be difficult without robust regulatory mechanisms.

In contrast, Algerian Law No. 18-07 does not explicitly define or regulate profiling or automated decision-making. Nevertheless, the law's core principles—such as the protection of human dignity, privacy, and public freedoms (Art. 2)—imply that any such processing must be transparent, lawful, and non-discriminatory. The data controller (responsable du traitement) is expected to ensure that individuals' rights are upheld and that safeguards are in place to prevent biased outcomes.

The ANPDP is empowered to oversee compliance, issue guidance, investigate complaints, and enforce corrective measures. While not as detailed as the GDPR, Law 18-07 demonstrates a legislative intent to regulate high-risk processing activities and protect individuals from automated systems that may infringe on their rights.

These core concepts will serve as reference points as we examine the broader challenges and legal approaches to data protection.

3. Global Challenges and Foundations of Data Protection

Data protection is shaped by global risks such as cyberattacks, data misuse, and privacy violations. This part outlines the ethical and strategic foundations of data privacy across sectors.

3.1 – Data Protection Principles (GDPR & Law 18-07)

Data protection legislation, both under the European General Data Protection Regulation and Algeria's Law No. 18-07, sets out a series of core principles that must govern all processing activities involving personal data. These principles, articulated in Article 5 of the GDPR and echoed in Articles 4 to 10 of Law 18-07, form the legal and ethical framework upon which all data processing operations must be based.

These principles are not optional or partial in their application; rather, they must be fully respected across all stages of data processing. A failure to comply with even one of them constitutes a violation of data protection law. For instance, retaining outdated information breaches the principle of accuracy, while collecting more data than necessary violates the principle of minimisation—even where consent was obtained.

It is important to distinguish the principle of lawfulness—which requires that all data processing be conducted in accordance with legal and ethical standards—from the specific legal justifications that make processing permissible. The latter, referred to as the "lawful bases for processing," will be examined in the following section.

The table below presents a comparative overview of these fundamental principles as they are defined and implemented under both legal frameworks, highlighting their shared structure, individual obligations, and legal foundations.

Table 1: data protection principles of Law 18-07 and GDPR

Principle	Definition	Key Regulatory Requirements	GDPR Ref.	Law 18-07 Ref.
Lawfulness, Fairness, and Transparency	Personal data must be processed based on a legitimate legal ground, in a fair manner that respects individuals' rights and freedoms, and with sufficient transparency to inform the data subject of the processing activities.	The controller must clearly disclose the identity of the data controller, purposes of processing, categories of data involved, and data subject rights, typically via a privacy notice.	Art. 5(1)(a)	Arts. 4–7
Purpose Limitation	Data must be collected for specified, explicit, and legitimate purposes and must not be further processed in a way incompatible with those original purposes.	Purposes must be determined at the time of data collection and documented. Further processing for secondary purposes requires either compatibility or a new legal basis.	Art. 5(1)(b)	Art. 8
Data Minimisation	The amount of personal data collected must be limited to what is strictly necessary in relation to the purposes for which it is processed.	The controller must justify each data field it collects and avoid collecting irrelevant or excessive information. Data collection must follow the principle of proportionality.	Art. 5(1)(c)	Art. 9
Accuracy	Personal data must be factually correct and, where necessary, kept up	Controllers must implement processes to ensure data accuracy and	Art. 5(1)(d)	Art. 9

	to date. Inaccurate or outdated data must be rectified or deleted without undue delay.	offer mechanisms for individuals to request correction of their information.		
Storage Limitation	Data should be retained only for as long as is necessary to fulfil the purposes for which it was collected.	Organizations must define and apply data retention periods, after which data is securely deleted, anonymised, or archived in compliance with legal and operational requirements.	Art. 5(1)(e)	Art. 10
Integrity and Confidentiality	Personal data must be processed in a manner that ensures its security, including protection against unauthorized access, loss, destruction, or damage.	Appropriate technical and organizational measures (such as encryption, access controls, and breach response protocols) must be in place to preserve data integrity and confidentiality.	Art. 5(1)(f)	Art. 10
Accountability	The data controller is not only responsible for complying with data protection principles but also for demonstrating such compliance to supervisory authorities and stakeholders.	This involves maintaining documentation, conducting risk assessments, training staff, and implementing internal governance mechanisms such as appointing a Data Protection Officer or Focal Point.	Art. 5(2)	Implied (Arts. 4–10)

Source : Author's elaboration based on (European Union, 2016, p. Art 5), (République Algérienne Démocratique et Populaire, 2018, pp. Art 4-10)

3.2 Lawful Bases for Data Processing

A fundamental requirement under data protection law is that all processing of personal data must be lawful. As defined in Article 5(1)(a) of the GDPR, lawfulness, fairness, and transparency constitute the first and overarching principle of data protection. However, the concept of **lawfulness** is further clarified in Article 6(1), which outlines six specific legal bases upon which personal data may be processed. These include consent, contractual necessity, legal obligation, protection of vital interests, performance of a task in the public interest or official authority, and legitimate interests.

In situations involving sensitive categories of data—such as health, religious affiliation, or biometric identifiers—additional safeguards are required under Article 9(2) GDPR. These conditions apply cumulatively and aim to protect data subjects from disproportionate risks associated with high-impact data processing.

Similarly, Algeria's Law 18-07 provides a legal framework that mirrors the GDPR in many respects, although with fewer distinctions between categories of data and fewer explicit lawful bases. The law places a strong emphasis on prior consent, legal obligation, and necessity, while delegating interpretive authority to the ANPDP for specific applications.

The table below provides a structured comparison of the legal grounds for data processing as established under the GDPR and Law 18-07, highlighting both convergence and areas of national specificity.

Table 2: Lawful Bases for Data Processing

Legal Basis	Definition	Key Regulatory Conditions	GDPR Ref.	Law 18-07 Ref.
Consent	A freely given, specific, informed, and unambiguous indication by which the data subject agrees to the processing of their personal data.	Consent must be obtained through a clear affirmative action, be documented, and remain withdrawable at any time. It must not be bundled with other agreements or implied through silence.	Art. 6(1)(a)	Arts. 4, 7
Contractual Necessity	Processing that is necessary to enter into or perform a contract with the data subject.	The processing must be directly linked to the execution or preparation of a contractual agreement with the individual concerned.	Art. 6(1)(b)	Art. 4
Legal Obligation	Processing that is necessary to comply with a legal obligation imposed on the data controller.	The obligation must derive from a specific law or regulation, and the controller must be able to demonstrate that the processing is required by that legal framework.	Art. 6(1)(c)	Art. 4
Vital Interests	Processing that is necessary to protect the life or physical integrity of the data subject or another person.	Used primarily in emergency scenarios, this basis applies when the data subject is incapable of giving consent and urgent intervention is needed.	Art. 6(1)(d)	Implicit
Public Interest / Official Authority	Processing necessary for the performance of a task carried out in the public interest or in the	The task must be established in law, and the processing must be necessary to fulfill that official function. Often	Art. 6(1)(e)	Art. 5

	exercise of official authority vested in the controller.	applicable to public bodies or state institutions.		
Legitimate Interests	Processing necessary for the purposes of the legitimate interests pursued by the controller or a third party, provided such interests are not overridden by the rights of the data subject.	Requires a case-by-case balancing test, weighing the interests of the controller against the privacy rights of individuals. Not applicable to public authorities acting in their official capacity.	Art. 6(1)(f)	Not explicitly addressed

Source : Author's elaboration based on (European Union, 2016, p. Article 6(1)),

3.3 Data Protection in a Digital World

In the digital era, data has become one of the most valuable resources for organizations, governments, and individuals alike. However, this growing reliance on data is accompanied by escalating concerns regarding privacy, misuse, and security breaches. The exponential growth of digital technologies—ranging from cloud computing to AI-driven analytics—has intensified the complexity of data protection and exposed critical vulnerabilities.

In the article "Privacy and Data Protection in the Digital Age," Gunuganti (2018) explores how traditional privacy norms are no longer sufficient in the digital environment. The regulatory frameworks that governed data in the early 2000s were built for static databases and simple client-server systems. Today, with dynamic data exchange between devices, platforms, and borders, these frameworks often fall short in ensuring effective protection. (Gunuganti, 2018)

One significant contribution of the article is its advocacy for Privacy by Design (PbD)—an approach that places privacy and security at the core of system design rather than treating them as afterthoughts. The PbD model emphasizes the minimization of personal data

collected, default privacy settings, user control over personal information, and secure data storage.

Figure 2: Steps to Ensure Data Privacy in the Digital Age

Source : (Gunuganti, 2018).

This figure outlines six key steps in ensuring privacy by design: data minimization, access limitation, transparency, secure infrastructure, accountability, and compliance monitoring. These principles help organizations embed privacy at every stage of data lifecycle management, fostering trust and regulatory compliance.

The article also draws attention to the fragmented nature of global data protection regulations. While the General Data Protection Regulation (GDPR) in the EU enforces strict rights for individuals and responsibilities for data processors, other regions adopt vastly different models. For instance, the U.S. approach tends to be sector-specific and market-driven, while China's model centers on state control and national security.

This diversity creates tension and uncertainty for global enterprises. Cross-border data flows often lead to legal conflicts and compliance challenges. Gunuganti argues that this legal inconsistency can only be resolved through international coordination and harmonization of standards.

Another critical theme is the so-called privacy paradox—a phenomenon in which individuals express concern over their personal data but frequently act in contradiction, sharing sensitive information on platforms like social media, e-commerce, or mobile apps. This paradox is further complicated by users' limited understanding of how their data is collected, stored, and exploited.

Figure 3: Factors Affecting Data Privacy

Source : (Gunuganti, 2018).

This visual model categorizes the various internal and external elements influencing data privacy: legal requirements, organizational culture, employee awareness, and technological infrastructure. It shows that data protection is not just a legal matter but a multidimensional challenge requiring coordinated efforts across technical, human, and regulatory domains.

Gunuganti concludes by emphasizing the need for a global digital ethics framework, one that balances innovation with responsibility. As data becomes increasingly commodified, protecting it must not rely solely on compliance but must also be embedded in corporate governance, product design, and user education.

In this context, data protection is more than a legal or technical obligation—it becomes a cornerstone of organizational resilience, user trust, and long-term strategic success. The following section will explore the potential consequences of poor data management, including reputational and operational risks.

3.4 Risks of Poor Data Management

In a digital economy where data serves as a strategic asset, poor data management poses significant threats that span operational, financial, ethical, and strategic dimensions. These risks arise from insufficient governance, fragmented systems, and lack of quality controls, ultimately undermining productivity, compliance, and decision-making capabilities (Redman, 1998).

1. Inaccurate Decision-Making

Decisions based on erroneous, outdated, or incomplete data can misguide forecasting, budgeting, and performance evaluation. This leads to resource misallocation, ineffective policies, and strategic misalignment across organizational functions.

2. Operational Inefficiencies

Data inconsistencies, duplicates, and formatting issues disrupt workflows and increase reliance on manual corrections. In data-intensive sectors such as healthcare or logistics, this reduces productivity and delays service delivery.

3. Financial Loss and Hidden Costs

Poor data quality generates both visible and hidden costs—ranging from failed transactions to misdirected marketing. It also undermines financial forecasting, cost control, and inventory management, creating inefficiencies that accumulate over time.

4. Damaged Reputation and Trust

Mishandled or inaccurate data can erode customer trust, damage brand reputation, and trigger regulatory scrutiny. Inaccurate billing, privacy violations, or public misstatements expose organizations to legal and reputational risks.

5. Security and Compliance Risks

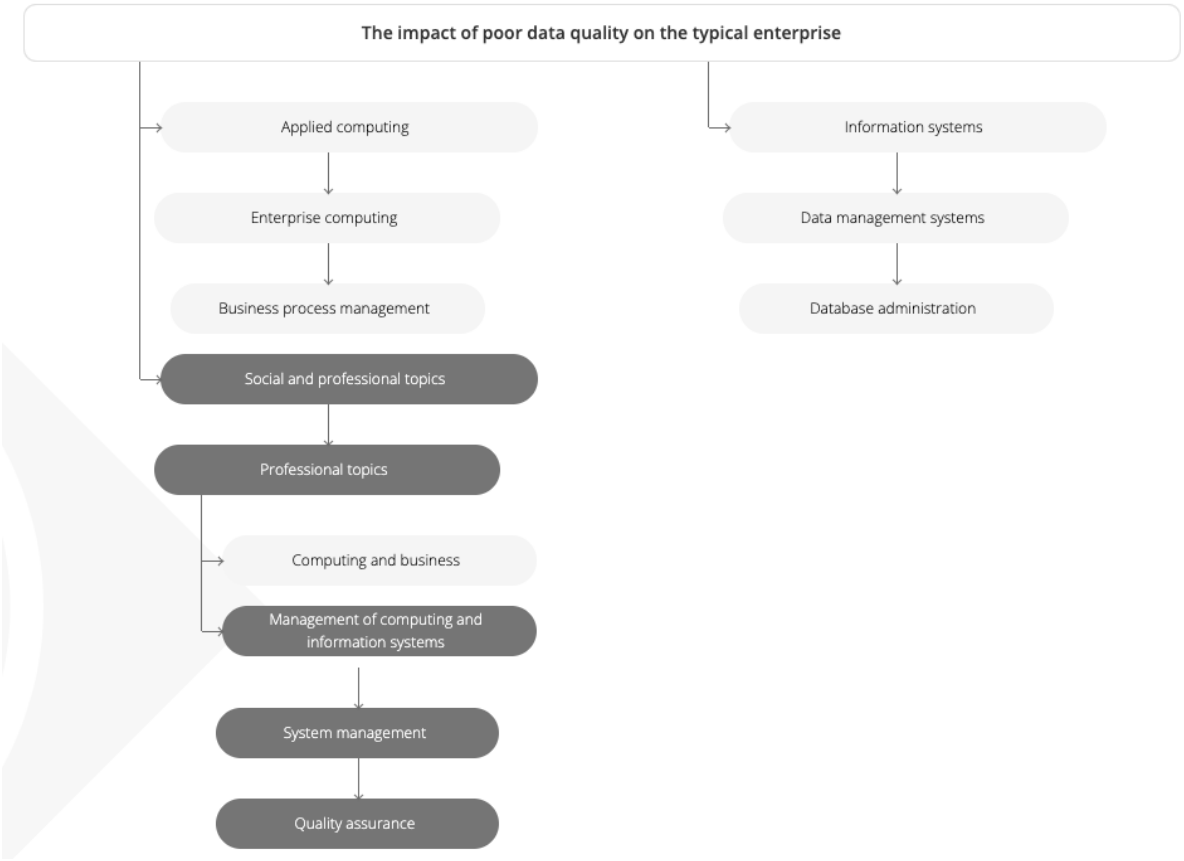
Inadequate classification, monitoring, or protection of data increases vulnerability to breaches and non-compliance. Weak governance structures and poor documentation hinder accountability and may result in legal sanctions under regulations such as the GDPR or Law 18-07.

6. Strategic Misalignment

Flawed data leads to strategic decisions that diverge from actual performance realities. This

weakens competitiveness, diverts investments, and impairs innovation and partnerships, reducing long-term value creation .

Figure 4: The Impact of Poor Data Quality on the Typical Enterprise



Source : (Redman, 1998)

Figure 4 illustrates the systemic nature of poor data quality and its cascading effects across both technical and managerial domains. On the technical side, deficiencies in data management systems and database administration serve as entry points for error propagation. These foundational flaws then extend upward, disrupting business process management, decision-making, and ethical responsibilities. The figure emphasizes that data quality is not confined to IT operations; it directly influences organizational accountability, strategic execution, and stakeholder trust. This visualization reinforces the idea that data quality is a cross-functional issue requiring integrated governance across departments.

In conclusion, poor data governance affects more than just technical systems—it disrupts strategic alignment, financial integrity, regulatory compliance, and organizational credibility.

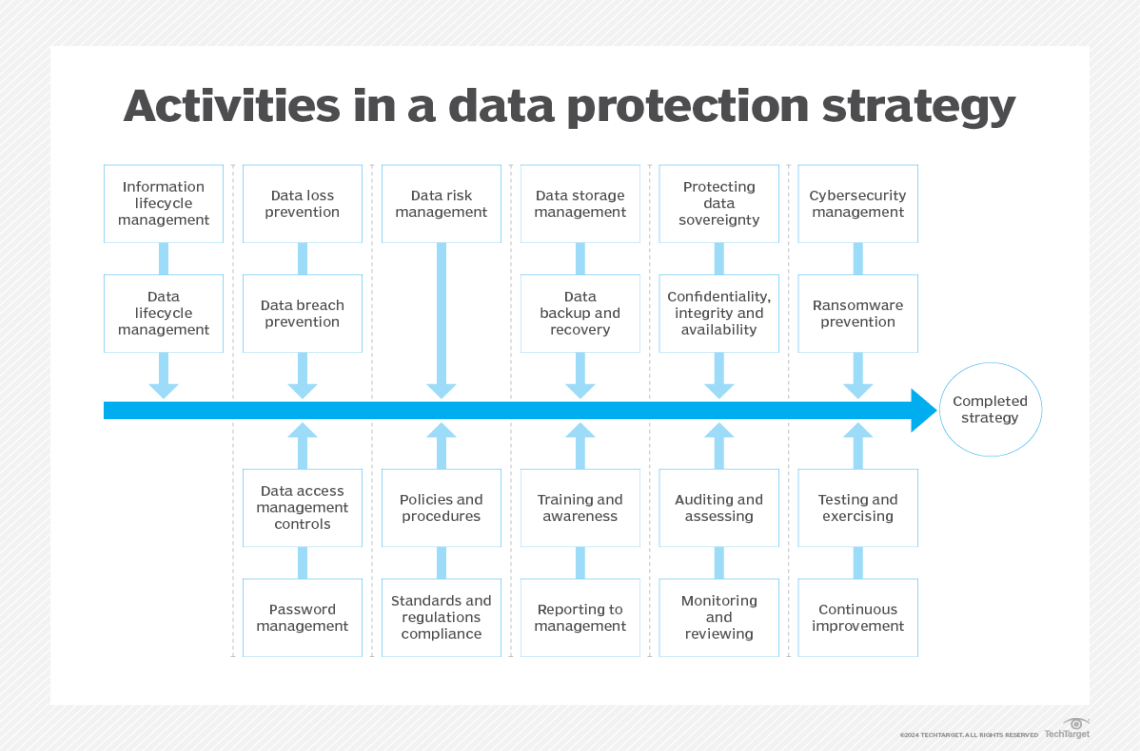
Addressing these risks requires structured data management frameworks and quality assurance protocols to enable responsible, efficient, and compliant use of data across all functions.

3.5 Strategic Importance of Data Protection

In today's data-centric environment, the protection of personal and organizational data has become a strategic imperative. According to Karjian (2024), data protection entails safeguarding data from loss, corruption, or unauthorized access, and ensuring that critical information can be recovered when needed. This function now extends beyond IT operations, influencing regulatory compliance, brand reputation, and innovation capacity.

One of the key aspects is business continuity and risk mitigation. Modern organizations must be prepared for cyberattacks, operational failures, or natural disasters. As illustrated in Figure 5 (Convergence of Backup and Disaster Recovery), traditional distinctions between backup and disaster recovery (DR) are narrowing, with integrated solutions designed to minimize downtime and ensure rapid restoration of systems (Karjian, 2024, p. 14).

Figure 5: Convergence of Backup and Disaster Recovery



Source : (Karjian, 2024, p. 14)

In parallel, regulatory compliance has become a major driver of data protection efforts. Frameworks such as the GDPR and CCPA require lawful and transparent data processing, with obligations relating to data minimisation, accountability, and the exercise of individual rights. Figure 6 helps clarify these overlapping concepts, distinguishing between availability (protection), confidentiality (privacy), and integrity (security) as distinct regulatory and operational goals (Karjian, 2024).

Figure 6: Data Protection vs. Privacy vs. Security

Source : (Karjian, 2024)

Another strategic pillar is consumer trust and brand reputation. Transparency in data handling practices—including clear privacy policies, informed consent, and respect for user rights—fosters credibility. The right to be forgotten, as enshrined in the GDPR, enhances public perception of ethical data stewardship and helps strengthen long-term customer relationships.

From a technological standpoint, data protection is closely tied to operational efficiency and digital innovation. Emerging technologies such as artificial intelligence, cloud computing, and Data Protection as a Service (DPaaS) offer scalable and cost-effective solutions. However, they also introduce new challenges, such as vendor dependency, bias in algorithmic systems, and opaque data flows—all of which must be addressed through robust governance (Karjian, 2024).

In sum, modern data protection is no longer confined to cybersecurity tools or compliance checklists. It is embedded in strategic planning and digital transformation. Organizations that

invest in comprehensive data protection frameworks—spanning governance, technology, and user engagement—gain a competitive advantage, reduce risk exposure, and build sustainable trust with stakeholders.

Understanding these global foundations allows us to better grasp the operational and legal responses detailed in the next section.

4. Personal Data Processing: Practices and Compliance

This section focuses on how personal data is processed, categorized, and regulated in practice. It reviews common processing activities and associated legal requirements.

4.1 What is Personal Data Processing?

Personal data processing refers to any action or set of actions performed on personal data, whether manually or through automated means. The European General Data Protection Regulation (GDPR), which sets the standard for personal data protection in the EU and influences global practices, defines processing under Article 4(2) as:

“Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (European Union, 2016, p. Article 4(2))

Similarly, Algeria’s Law No. 18-07 of 10 June 2018, which governs the protection of individuals with regard to the processing of personal data, offers an almost identical legal definition in Article 3. In French, the law states:

« Toute opération ou ensemble d'opérations, effectuées ou non à l'aide de procédés automatisés, appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. » (République Algérienne Démocratique et Populaire, 2018, p. art. 3)

Its official English translation reads:

"Any operation or set of operations, whether or not by automated means, applied to personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

This broad definition ensures that nearly all activities involving personal data—whether accessing a file, modifying a record, or even erasing it—fall under the regulatory scope. Notably, both the GDPR and Law 18-07 emphasize that the technology or format used (digital or paper-based) is irrelevant so long as the data is part of a structured filing system. Processing can be done by data controllers (who define the purpose and means) or data processors (who act on behalf of the controller).

The legal basis for processing is also crucial. If the original basis is consent, it must be renewed for any new purpose, especially in contexts like scientific research, unless the data is anonymized. Consent must be specific and informed; therefore, using data for a new purpose without renewed consent may violate the initial agreement. However, when data is effectively anonymized, it is no longer considered personal and falls outside the scope of data protection laws.

In research, "broad consent" may be acceptable under Recital 33 of the GDPR, which allows individuals to give consent to general areas of scientific inquiry, provided that ethical standards are met. This offers a degree of flexibility when specific research goals cannot be fully determined at the time of data collection. Nevertheless, where possible, individuals should be given granular options to consent only to certain aspects or areas of the research (European Union, 2016, p. Recital 33).

Understanding this concept is essential for ensuring the lawful and ethical handling of personal data in both digital and non-digital contexts.

4.2 Types of Processing Activities

In both the GDPR and Algeria's Law No. 18-07, the concept of personal data processing is defined in a broad and inclusive manner. Article 4(2) of the GDPR and Article 3 of Law 18-07 encompass a wide range of operations—including collection, recording, structuring, storage, consultation, disclosure, and erasure—regardless of whether the processing is automated or manual. These operations can be grouped into six functional categories, reflecting the typical data lifecycle: (1) collection, (2) structuring, (3) storage and retention, (4) use and consultation, (5) disclosure, and (6) erasure or destruction.

Each of these categories involves distinct responsibilities for data controllers and processors. Data may be collected through various channels (e.g., forms, sensors, digital platforms), then recorded and structured within information systems. Once stored, it is used or accessed for specific purposes and may be disclosed to third parties such as service providers or public institutions. Finally, when no longer necessary, personal data must be securely deleted or destroyed.

This classification, which mirrors both European and Algerian legal definitions, is essential for documenting processing operations, assessing legal obligations, and implementing data protection principles such as purpose limitation, data minimisation, and storage limitation.

Table 3: Summary of Personal Data Processing Activities

Category	Description
Collection	Gathering personal data from sources like forms, surveys, or web interactions.
Recording	Capturing and entering data into structured systems.
Organisation and Structuring	Systematically arranging data for efficient access and analysis.
Storage	Preserving data in physical or electronic environments.
Adaptation or Alteration	Modifying or updating data to ensure accuracy.
Retrieval and Consultation	Accessing and reviewing data when necessary.

Use	Utilizing data for specific purposes, such as services or research.
Disclosure / Transmission	Sharing data with third parties via digital or manual means.
Alignment / Combination	Integrating data from multiple sources to enrich datasets.
Restriction	Temporarily or permanently limiting access or processing under specific rules.
Erasure or Destruction	Securely deleting or physically destroying data no longer needed.

Source : Author's elaboration based on (European Union, 2016, p. Article 4(2))and (République Algérienne Démocratique et Populaire, 2018, p. Article 3).

These activities can be executed through automated systems (e.g., software, algorithms) or manual methods (e.g., paper filing). The GDPR and Law 18-07 both apply to automated and manual processing when personal data is part of a structured filing system.

In sum, a comprehensive understanding of the different types of personal data processing activities is fundamental for organizations aiming to ensure compliance with both international and national data protection frameworks. From collection to final erasure, each phase introduces specific legal, technical, and organizational responsibilities. Recognizing these categories not only facilitates the proper documentation and oversight of processing operations but also lays the groundwork for the effective application of privacy principles such as lawfulness, purpose limitation, and data minimization.

Building on this foundational knowledge, the next section will explore how these data protection principles are practically applied within each processing activity, providing real-world insights into compliant and ethical data management practices.

4.3 Practical Application of Data Protection Principles in Processing

Ensuring that personal data processing not only complies with statutory requirements but also respects individuals' rights demands the concrete integration of core data protection principles into everyday operations. Both the European General Data Protection Regulation (GDPR) and Algeria's Law No. 18-07 enshrine a set of foundational imperatives—lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, security, and accountability—which must guide every phase of the data lifecycle, from collection through to erasure (European Union, 2016, p. Art. 4)

At the outset, lawfulness, fairness, and transparency require that each processing activity rest on a clearly established legal basis—whether consent, contractual necessity, or a statutory obligation—and that data subjects are fully informed of how and why their data will be used. In practice, organizations meet this obligation by publishing concise privacy notices and obtaining unambiguous, freely given consent where required (European Union, 2016, p. Art. 4)

The principles of purpose limitation and data minimization work in tandem: data may only be collected for explicit, legitimate purposes and must be limited to what is strictly necessary to achieve those purposes. Operationalizing this means designing forms and systems to capture only essential fields, and regularly reviewing data inventories to delete or anonymize elements no longer needed (European Union, 2016, pp. Art. 5(1)(b)–(c))

Maintaining accuracy and enforcing storage limitation obliges organizations to implement processes for data verification and to establish retention schedules aligned with legal or business requirements. Automated validation checks, periodic audits, and secure disposal protocols help prevent the risks posed by outdated or excessive data holdings (European Union, 2016, p. Art. 4)

Security (integrity and confidentiality) extends beyond technical measures—such as encryption, access controls, and intrusion detection—to include physical safeguards and staff training. In Algeria, the Autorité nationale de protection des données à caractère personnel (ANPDP) monitors the adequacy of such measures, requiring organizations to demonstrate that they have adopted "appropriate technical and organizational measures" against unauthorized or unlawful processing (République Algérienne Démocratique et Populaire, 2018, p. Art. 4)

Finally, accountability transforms these abstract principles into tangible obligations. Data controllers must maintain comprehensive Records of Processing Activities (RoPA), conduct Data Protection Impact Assessments (DPIAs) for high-risk operations, and appoint Data Protection Officers (DPOs) when mandated by the nature or scale of processing (Regulation (EU) 2016/679, Arts. 30, 35–37). In Algeria, although the formal requirement to appoint a DPO is not yet codified, Law 18-07 obliges controllers to cooperate fully with the ANPDP and to provide evidence of compliance upon request (République Algérienne Démocratique et Populaire, 2018, p. Art. 12).

By embedding these principles into system design, policy frameworks, and everyday workflows, organizations can ensure that processing activities remain both legally sound and ethically robust. The following section will illustrate how data protection principles translate into concrete measures—such as privacy by design, consent management platforms, and breach response protocols—thereby closing the gap between regulatory theory and operational practice.

4.4 – Rights of the Data Subject

The legal framework for data protection under both the GDPR and Algeria's Law No. 18-07 is fundamentally rooted in the rights granted to individuals, referred to as data subjects. These rights aim to ensure transparency, fairness, and control over the use of personal data, reinforcing accountability on the part of data controllers. While the GDPR provides an extensive and detailed list of rights through Articles 12 to 22, Algeria's Law No. 18-07 incorporates many of these protections, albeit with varying levels of specificity and legal precision. The table below presents a comparative analysis of these rights as recognized under both frameworks.

Table 4: comparative analysis of the rights of the data subject

Right	GDPR Reference	Definition under GDPR	Recognition in Law 18-07	Observations
Right to Information	Articles 12–14	The right to be informed about the collection, purpose, legal basis,	Recognized	Individuals must be informed clearly and comprehensively

		recipients, and retention of personal data, along with data subject rights.		before or at the time of data collection.
Right of Access	Article 15	The right to obtain confirmation that data is being processed and to access one's personal data and associated processing information.	Recognized	Law 18-07 guarantees access to personal data and related details held by controllers.
Right to Rectification	Article 16	The right to have inaccurate personal data corrected or completed if it is incomplete.	Recognized	Similar provision exists, enabling correction or updating of inaccurate data.
Right to Erasure ("Right to be Forgotten")	Article 17	The right to request deletion of personal data when it is no longer necessary, unlawfully processed, or withdrawn by consent.	Recognized	Deletion is permitted, especially for outdated or unlawfully processed data.
Right to Object	Article 21	The right to object to processing, particularly for direct marketing or where processing is based on legitimate interests.	Recognized	Data subjects may object to processing, especially for marketing or other legitimate concerns.
Right to Restrict Processing	Article 18	The right to request restriction of processing under specific conditions (e.g. contesting data accuracy).	Implicit	Not explicitly provided, but inferred from provisions on objection and data accuracy.

Right to Data Portability	Article 20	The right to receive personal data in a structured, commonly used, machine-readable format and transfer it to another controller.	Not Recognized	No explicit equivalent under Law 18-07. May represent a future area of legal development.
Rights related to Automated Decision-Making and Profiling	Article 22	The right not to be subject to decisions based solely on automated processing, including profiling, that significantly affects the individual.	Not Recognized	No specific provision. Indicates a legislative gap regarding AI and profiling practices.

Source : Author's elaboration based on (European Union, 2016, p. Articles 12 to 22).

While the two legal frameworks share a strong alignment on fundamental rights such as access, rectification, and erasure, the GDPR provides a more detailed and enforceable structure, particularly with regard to data portability and automated decision-making. These differences reflect the evolving nature of digital governance and highlight potential directions for legislative enhancement under Algerian law 18-07.

A clear understanding of these practices enables us to assess how international legal frameworks have adapted to modern data ecosystems.

Section 2 : Legal Framework and International Comparison

To ensure privacy, various legal systems have adopted structured regulations. This section compares major frameworks such as the GDPR and other national laws.

1. Overview of Law 18-07 and the Algerian Legislative Framework

Enacted on June 10, 2018, Law No. 18-07 represents Algeria's first comprehensive legal framework dedicated to personal data protection. It aligns the country with international data privacy standards, particularly in response to the expansion of digital services, cloud computing, and mass data collection across sectors (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025)

The primary objective of Law 18-07 is to safeguard the rights and freedoms of individuals in a context of rapid digital transformation. It aims to ensure transparency**,** accountability, and lawful processing, assigning legal responsibility to all entities that process personal data within Algeria or target Algerian citizens. The law also seeks to foster digital trust, limit abusive data practices (e.g. surveillance or unauthorized sharing), and support the development of a secure and innovation-friendly digital economy (CNIL & Délégation Algérienne, 2021).

These goals are part of Algeria's broader national digital strategy, which promotes public service modernization and entrepreneurship in the digital sector (Ministère de la Numérisation, 2022). An infographic (Figure 7) summarizes the core data protection principles under Law 18-07, such as confidentiality, legality, and individual rights protection—designed to promote responsible and ethical data governance. (Marketing Intervalle, 2024)

Figure 7: fundamental principles of data protection

Source : (Marketing Intervalle, 2024)

❖ **Scope of Application**

Law 18-07 applies to all personal data processing carried out by public or private entities in Algeria, using either automated or manual means. Its jurisdiction also extends to foreign organizations processing the data of Algerian residents. It covers a wide range of sectors including health, finance, telecommunications, and e-commerce. Specific provisions apply to **sensitive data** (e.g., biometric, health, religious), which require prior authorization from the national authority.

❖ **Legal Obligations for Controllers and Processors**

The law imposes several key obligations on data controllers and processors:

- **Declaration and Authorization** of processing activities, especially for sensitive data, to the national authority (ANPDP);
- **Informed Consent** that is explicit, specific, and freely given by the data subject;
- **Data Minimization and Purpose Limitation**, ensuring that data collected is relevant, necessary, and lawfully justified;

- **International Data Transfer Restrictions**, only permitted with adequate safeguards or ANPDP approval;
- **Security Measures** including encryption, access control, and regular audits;
- **Respect for Data Subject Rights**, such as access, rectification, deletion, and objection to processing.

Non-compliance with these obligations may lead to **administrative sanctions or criminal liability**, particularly in cases involving the unauthorized processing or disclosure of sensitive personal data.

❖ **Integration within the National Legal Framework**

Law 18-07 complements other national legislation, including **Law No. 05-20** on electronic transactions and penal code provisions related to cybercrime. Collectively, these laws support the creation of a safe digital environment for both public and private sector innovation.

However, as of 2022, the **ANPDP** remains non-operational, limiting the enforcement of Law 18-07. Despite this institutional delay, the law places Algeria among countries actively developing data protection regimes, reflecting a growing institutional commitment to digital rights and regulatory modernization.

2. Comparison with International Standards

This part offers a focused comparison between Algeria's Law 18-07 and international standards like the GDPR and ISO 27701. The goal is to assess compatibility and identify gaps.

2.1 The GDPR: General Data Protection Regulation

The General Data Protection Regulation (GDPR), formally known as Regulation (EU) 2016/679, is a comprehensive legal framework enacted by the European Union to safeguard individuals' personal data and privacy. Adopted in April 2016 and enforced since May 25, 2018, the GDPR replaces the 1995 Data Protection Directive, aiming to harmonize data protection laws across EU member states and enhance individuals' control over their personal information. (European Union, 2016).

- **Scope and Applicability**

The GDPR applies to all organizations operating within the EU, as well as to entities outside the EU that offer goods or services to, or monitor the behavior of, EU data subjects. This extraterritorial applicability ensures that any organization processing the personal data of individuals within the EU complies with the regulation, regardless of the organization's location (European Commission)

- **Key Principles**

The regulation is founded on several core principles that govern the processing of personal data:

- **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation**: Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization**: Processing should be adequate, relevant, and limited to what is necessary concerning the purposes for which data are processed.
- **Accuracy**: Personal data must be accurate and, where necessary, kept up to date.

- **Storage Limitation**: Data should be kept in a form that permits identification of data subjects for no longer than necessary.
- **Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- **Accountability**: The data controller is responsible for, and must be able to demonstrate, compliance with these principles.

❖ **Data Subject Rights**

The GDPR grants individuals several rights concerning their personal data:

- **Right of Access**: Individuals can obtain confirmation as to whether their data is being processed and access to that data.
- **Right to Rectification**: Individuals can have inaccurate personal data corrected.
- **Right to Erasure ("Right to be Forgotten")**: Individuals can have their personal data erased under certain conditions.
- **Right to Restrict Processing**: Individuals can request the restriction of processing under specific circumstances.
- **Right to Data Portability**: Individuals can receive their personal data in a structured, commonly used, and machine-readable format and have the right to transmit that data to another controller.
- **Right to Object**: Individuals can object to the processing of their personal data in certain situations.
- **Rights Related to Automated Decision Making and Profiling**: Individuals have rights concerning automated decisions, including profiling, that significantly affect them (European Commission).

❖ Obligations for Data Controllers and Processors

Organizations subject to the GDPR must adhere to various obligations

- **Data Protection by Design and by Default**: Implement appropriate technical and organizational measures to ensure data protection principles are integrated into processing activities.
- **Data Protection Impact Assessments (DPIAs)**: Conduct assessments for processing operations that are likely to result in high risks to individuals' rights and freedoms.
- **Appointment of Data Protection Officers (DPOs)**: Designate DPOs in certain circumstances, such as when processing is carried out by public authorities or involves large-scale processing of special categories of data.
- **Breach Notification**: Notify the relevant supervisory authority of personal data breaches within 72 hours of becoming aware, unless the breach is unlikely to result in a risk to individuals' rights and freedoms.

❖ Enforcement and Penalties

Non-compliance with the GDPR can result in significant penalties. Organizations may face administrative fines of up to €20 million or 4% of their total global annual turnover, whichever is higher, depending on the nature and severity of the infringement (European Commission).

Table 5: GDPR vs. Algeria's Law No. 18-07

Criteria	GDPR (EU)	Law No. 18-07 (Algeria)
Date of Adoption	Adopted on April 27, 2016; enforced from May 25, 2018.	Adopted on June 10, 2018; enforcement commenced on August 10, 2023.
Territorial Scope	Applies to all EU member states and to organizations outside the EU that process personal data of individuals within the EU.	Applies to the processing of personal data by public and private entities within Algeria.

Legal Basis for Processing	Processing is lawful if based on consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests.	Processing requires prior declaration or authorization by the national authority; consent is a primary basis, with exceptions for public interest or legal obligations.
Key Principles	Lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.	Lawfulness, fairness, transparency, purpose specification, data minimization, accuracy, storage limitation, and security.
Data Subject Rights	Right to be informed, access, rectification, erasure, restriction of processing, data portability, objection, and rights related to automated decision-making.	Right to be informed, access, rectification, opposition, and erasure; no explicit mention of data portability or automated decision-making rights.
Sensitive Data Processing	Special categories of data (e.g., racial or ethnic origin, political opinions, religious beliefs) require explicit consent or specific legal grounds.	Processing of sensitive data is prohibited unless authorized by the national authority or justified by public interest, medical purposes, or legal obligations.
Data Protection Officer (DPO)	Mandatory appointment for certain organizations, especially those processing large-scale sensitive data.	No explicit requirement for DPO appointment; however, data controllers must ensure compliance with the law.
Data Breach Notification	Mandatory notification to supervisory authority within 72 hours of becoming aware of a breach; affected individuals must also be informed without undue delay.	Service providers must notify the national authority and affected individuals without delay in case of breaches in public electronic communication networks.

Cross-border Data Transfers	Permitted to countries with adequate data protection levels or through mechanisms like Standard Contractual Clauses.	Transfers require authorization from the national authority and are permitted if the recipient country ensures adequate data protection.
Supervisory Authority	Independent national data protection authorities in each member state, coordinated by the European Data Protection Board (EDPB).	National Authority for the Protection of Personal Data (ANPDP), an independent body under the President's authority.
Sanctions and Penalties	Administrative fines up to €20 million or 4% of global annual turnover, whichever is higher.	Administrative fines up to DZD 500,000 (~€3,100); criminal penalties include imprisonment ranging from two months to five years and fines up to DZD 500,000.
Accountability and Documentation	Data controllers must maintain records of processing activities and demonstrate compliance with GDPR principles.	Data controllers are required to declare processing activities to the national authority and ensure compliance with the law.
Data Protection Impact Assessments (DPIAs)	Mandatory for high-risk processing activities to assess and mitigate risks to data subjects.	No explicit requirement for DPIAs; however, prior authorization is needed for certain processing activities.
Children's Data	Specific provisions for processing children's data, including obtaining parental consent for those under 16.	Requires prior consent from legal guardians or judicial authorization for processing children's data.
Direct Marketing	Requires explicit consent; data subjects have the right to object to direct marketing.	Direct marketing is generally prohibited unless specific conditions are met and authorized by the national authority.

Automated Decision-Making and Profiling	Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling.	No explicit provisions regarding automated decision-making or profiling.

Source : Author's elaboration based on the GDPR and Law 18-07 .

2.2 ISO 27701: A Framework for Privacy Management

ISO/IEC 27701 is an international privacy standard developed as an extension to ISO/IEC 27001 and ISO/IEC 27002. It provides guidelines for establishing, maintaining, and continuously improving a Privacy Information Management System (PIMS) (International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2019). Its main goal is to help organizations comply with data protection regulations such as the GDPR, CCPA, and national laws like Algeria's Law No. 18-07.

This standard defines requirements and controls for both data controllers and data processors, focusing on transparency, accountability, documentation, and risk management in handling personally identifiable information (PII). It emphasizes privacy by design, security controls, and clearly documented responsibilities. The following table outlines the key differences and similarities between ISO/IEC 27701 and Algeria's Law 18-07:

Table 6: key differences and similarities between ISO/IEC 27701 and Algeria's Law 18-07.

Criterion	ISO/IEC 27701	Algerian Law No. 18-07
Legal Nature	Voluntary international standard	Mandatory national legislation
Scope	Information security + privacy management	Personal data protection
Target Audience	Organizations seeking certification or compliance alignment	All entities processing data of Algerian residents

Roles Defined	Controller, Processor, PIMS Manager	Data Controller (Responsable du traitement), Processor (Sous-traitant)
Risk Management	Requires Privacy Impact Assessments (PIAs)	Authorizations required for sensitive data processing
Certification	Can be audited and certified	No certification mechanism yet under Law 18-07
Supervisory Body	None – relies on third-party audits	National Authority (ANPDP)
Implementation Tools	Detailed operational and documentation requirements	Legal principles, authorizations, and compliance mechanisms

Source : Author's elaboration based on (International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2019) and (République Algérienne Démocratique et Populaire, 2018).

While ISO/IEC 27701 offers an operational framework for managing privacy risks, Algeria's Law 18-07 establishes a legal structure with regulatory oversight. ISO 27701 can support compliance with Law 18-07 by helping organizations implement technical and organizational measures aligned with international best practices.

Although ISO/IEC 27701 is not legally binding, it provides organizations with a structured, auditable approach to managing privacy obligations. For Algerian companies, adopting ISO 27701 may strengthen their compliance posture under Law 18-07, particularly in the absence of detailed regulatory guidance. Its adoption also enhances trust, transparency, and cross-border data governance, making it a useful complement to national law.

The findings reveal both areas of convergence and the need for stronger implementation tools—especially at the institutional level

3. The Role of the ANPDP as a Regulatory Authority

Effective data protection relies on oversight. This section explores the structure and expected functions of Algeria's supervisory authority, the ANPDP.

3.1 Main Missions and Responsibilities

The National Authority for the Protection of Personal Data is the principal Algerian regulatory body responsible for overseeing and ensuring the lawful, ethical, and secure processing of personal data. As outlined in Presidential Decree No. 22-187 of May 18, 2022, the ANPDP is an independent administrative authority *endowed with* legal personality *and* financial and administrative autonomy. Its mandate is to guarantee the respect for human dignity, individual freedoms, and private life during the processing of personal data across all sectors, both public and private. The ANPDP's headquarters is located in Hydra, Algiers, and its governing body is composed of 16 members, including its president, appointed by presidential decree for a five-year term (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

The establishment of the ANPDP reflects Algeria's commitment to aligning its legal framework with international standards of data protection, such as the General Data Protection Regulation (GDPR) in the European Union. This institutional structure plays a central role in ensuring the effective implementation of Law 18-07 of June 10, 2018, which governs the protection of individuals concerning the processing of personal data.

3.2 Structure and Functions of the Executive Secretariat

The Executive Secretariat of the ANPDP operates as the central executive arm responsible for implementing and coordinating the Authority's decisions and regulatory missions. According to Article 1 to Article 13 of Decree No. 23-73, the Executive Secretariat is established to ensure that the Authority's policies and oversight functions are executed efficiently across administrative, technical, and legal levels (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

❖ Legal Mandate and Governance

As per Article 1 of the decree, the Executive Secretariat functions within the scope of Law 18-07, and under the direct supervision of the President of the ANPDP. It operates as the central logistical and operational structure tasked with executing regulatory, administrative, and strategic objectives related to personal data protection.

❖ Key Missions and Functions

Outlined in Article 4 and Article 5, the main responsibilities of the Executive Secretariat include:

- **Authorization Management**: Receiving, examining, and processing requests for authorizations and licenses related to the processing of personal data, particularly when such processing involves sensitive or cross-border elements.
- **Complaints and Appeals Handling**: Receiving, registering, and investigating complaints and grievances from data subjects or legal entities regarding breaches of data protection rules, and preparing appropriate follow-up reports.
- **Communication and Notifications**: Ensuring the communication of the Authority's decisions, opinions, and notifications to concerned individuals, institutions, or regulatory bodies.
- **Supervision of Enforcement**: Monitoring and following up on the implementation of the decisions issued by the Authority, including initiating corrective measures in case of non-compliance.
- **Support for Internal Operations**: Assisting the President in the day-to-day administration and financial management of the Authority, including preparation of meeting agendas, reports, and official records.
- **Preparation of Regulatory and Administrative Reports**: Drafting reports on licensing, investigations, inspections, public consultations, and legal recommendations for the President and the Authority's board.
- **Managing Public Inquiries and Submissions**: Preparing summaries, response letters, and legal recommendations for external requests (including data transfer authorizations and privacy concerns from foreign entities).

- **Technical Evaluation and Compliance Audits**: Implementing technical audits, compliance checks, and developing risk-based control programs in collaboration with legal and technical departments. (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

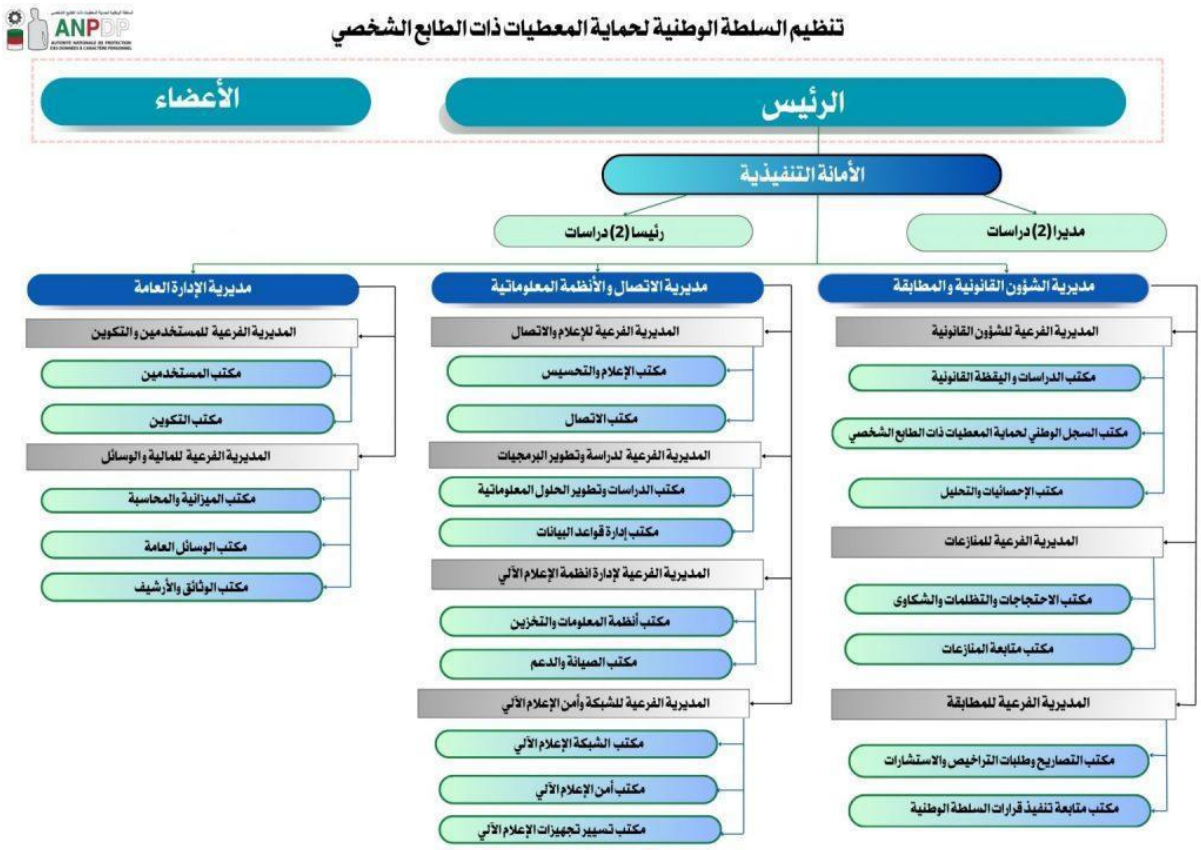
❖ **Internal Composition of the Executive Secretariat**

As per Articles 6–10, the Secretariat is structured into three key directorates, each responsible for specialized domains:

1. **The Directorate of Legal and Compliance Affairs**
    - Oversees legal studies and ensures alignment of ANPDP actions with national and international laws.
    - Handles dispute resolution, license preparation, and follow-up on judicial matters.
    - Conducts legal monitoring and contributes to national regulatory reforms.
2. **The Directorate of Information Systems and Communications**
    - Maintains the Authority's IT infrastructure, digital platforms, and online communications.
    - Ensures cybersecurity, data center security, system updates, and network integrity.
    - Prepares and implements digital tools and applications for regulatory use (e.g., case tracking, data registries).
    - Oversees the Authority's online presence and digital awareness initiatives.
3. **The Directorate of General Administration**
    - Manages human resources, recruitment, training programs, budgeting, procurement, and material resources.
    - Prepares internal logistics, including office equipment, technical maintenance, and organizational planning.
    - Oversees internal communications and the preservation of administrative archives and documents.

Each directorate includes sub-directorates (services) specialized in technical development, communication, training, auditing, and legal affairs, enabling comprehensive support for the Authority's core functions (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

Figure 8: Organizational Structure of the ANPDP



Source : (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025)

The figure illustrates the hierarchy and functional division within the ANPDP, from its President at the top, down through the Executive Secretariat and its three main directorates. Each directorate contains functional departments specialized in legal compliance, information systems, administrative support, communication, auditing, and training. This structure allows for multidisciplinary coordination and agile governance across complex regulatory domains.

❖ **Operational Integration and Strategic Oversight**

The Executive Secretariat functions under the supervision of the ANPDP President**,** ensuring horizontal coordination between directorates and alignment with the Authority's annual strategy. The President delegates responsibilities to the Secretariat to streamline operational processes and enforce the Authority's decisions effectively across all regulated entities.

The Secretariat also contributes to annual reporting**,** public communication strategies**,** and the implementation of national data protection campaigns**,** reflecting its role not only as an administrative body but also as a driver of regulatory education and outreach.

3.3 Guidance for Companies on Compliance

To assist organizations in aligning with Law No. 18-07 concerning the protection of personal data, the ANPDP offers a comprehensive suite of tools and resources. These are designed to facilitate compliance and ensure that data processing activities respect individuals' rights and privacy.

A. Compliance Procedures and Training Guides

The ANPDP provides a dedicated portal featuring various resources to guide organizations through the compliance process:

- **Compliance Procedures**: Detailed steps outlining how organizations can align their data processing activities with legal requirements.
- **Prototypes and Templates**: Standardized documents and forms to assist in the documentation and implementation of data protection measures.
- **Training Guides**: Educational materials aimed at raising awareness and understanding of data protection principles among staff and stakeholders.

These resources are accessible via the ANPDP's official website (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

B. User Manual for Online Services

To streamline interactions with the ANPDP, a comprehensive user manual is available, detailing the use of the online portal. This includes:

- **Account Creation**: Guidance on setting up an account for data controllers.
- **Declarations and Authorizations**: Instructions for submitting data processing declarations and authorization requests.
- **Consultation Requests**: Procedures for seeking advice or opinions from the ANPDP.
- **Appointment Scheduling**: Steps to book appointments for dossier submissions (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

C. Communication Mechanisms

The ANPDP maintains open channels of communication to support organizations:

- **Official Website**: Regular updates, resources, and announcements.
- **Email Support**:
  - **General Inquiries**: contact.anpdp@anpdp.dz
  - **Legal Questions**: questions.juridiques@anpdp.dz
  - **Technical Support**: questions.techniques@anpdp.dzanpdp.dz
- **Telephone**: +213 (23) 477 300 (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

These channels ensure that organizations can seek guidance and clarification as needed.

D. Training and Awareness Initiatives

Recognizing the importance of education in data protection, the ANPDP offers:

- **Training Sessions**: Workshops and seminars tailored to different sectors and organizational needs.
- **Awareness Campaigns**: Initiatives aimed at promoting best practices in data handling and processing.

These programs are designed to enhance understanding and implementation of data protection measures across organizations.

E. Audit Manual and Compliance Framework

To assist organizations in evaluating their compliance status, the ANPDP provides:

- **Audit Manuals**: Guidelines for conducting internal audits of data processing activities.
- **Compliance Frameworks**: Structured approaches to identify and address potential gaps in data protection practices.

These tools are instrumental in fostering a culture of continuous improvement and adherence to legal standards.

The authority's design is promising but its delayed operationalization limits enforcement—leading us to the operational aspects of the legal framework.

These international models set the stage for a closer look at how Algerian law aligns—or diverges—from global standards (Autorité nationale de protection des données à caractère personnel [ANPDP], 2025).

Section 3 : Mapping Law 18-07: Legal Architecture of Personal Data Protection and Processing

This final theoretical section visualizes the legal and operational logic of data protection. It maps relationships between legal actors, obligations, and individual rights.

1. Structural Overview of Law 18-07

Law No. 18-07 of 10 June 2018 establishes Algeria's legislative foundation for the protection of personal data. Its structure reflects a comprehensive and methodical organization, ensuring that both the rights of individuals and the responsibilities of data controllers are systematically addressed. The law is composed of **seven main titles**, each encompassing specific thematic areas—from general provisions to sanctions and the functioning of the supervisory authority (ANPDP). This section provides a high-level structural cartography of the law, without repeating analytical content already discussed in previous sections.

❖ Overall Architecture of Law 18-07

The law is composed of **74 articles** organized into the following **seven titles**, each addressing a fundamental pillar of personal data protection:

Table 7: the 7 principle titles of the law 18-07 .

Title	Theme	Articles
I	General Provisions	1–6
II	Conditions of Lawful Processing	7–16
III	The National Authority for Data Protection (ANPDP)	17–28
IV	Rights of the Data Subject	29–41
V	Rules on International Data Transfers	42–47
VI	Organizational Provisions of the Authority	48–59
VII	Offences and Sanctions	60–74

Source : Author’s elaboration based on (République Algérienne Démocratique et Populaire, 2018).

❖ Purpose of This Legal Structure

The structural segmentation of the law is not arbitrary—it reflects a logic of progression:

- **Titles I–II** define the legal bases and principles of processing.
- **Title III** institutionalizes oversight and compliance mechanisms via the ANPDP.
- **Title IV** guarantees the individual rights of citizens over their data.
- **Titles V–VI** operationalize control, especially in cross-border contexts.
- **Title VII** provides enforcement tools through administrative and criminal sanctions.

This modular structure allows both public and private stakeholders to navigate obligations effectively and ensures that each legal actor can identify the relevant articles depending on their role (data controller, processor, subject, or supervisory entity), (République Algérienne Démocratique et Populaire, 2018) .

2. Thematic Mapping of Key Provisions

This subsection aims to reorganize the legal content of Law 18-07 around six major functional themes instead of the law's original order. This mapping helps visualize how the law regulates protection and processing, and how its different parts interact to form a coherent legal regime.

A. Fundamental Protection Principles

These articles define the ethical and legal foundations of personal data protection.

Table 8: Ethical and legal foundations of personal data protection

Key Concepts	Articles	Summary
Respect for human dignity	Art. 2	Data processing must respect the dignity and private life of individuals.
Principles of legality, purpose, proportionality, and minimization	Art. 4–6	Processing must have a lawful basis, respect a defined purpose, and use only necessary data.

Legal bases for processing	Art. 7–10	Covers consent, legal obligation, contract, public interest, or vital interests.
Special categories of data	Art. 8–9	Sensitive data (e.g., health, religion, biometrics) requires enhanced protection.

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018).

B. Rights of Data Subjects

These provisions secure individuals' control over their own data.

Table 9: Rights of data subjects in Law 18-07 .

Right	Articles	Details
Right to information	Art. 17	Individuals must be informed about data collection and usage.
Right of access	Art. 32	Citizens can request and review personal data held about them.
Right to rectification	Art. 34	Inaccurate or incomplete data must be corrected.
Right to erasure ("right to be forgotten")	Art. 36	Under specific circumstances, individuals can demand deletion of their data.
Right to object	Art. 35	Individuals can oppose data processing under certain conditions.
Right to complaint or appeal	Art. 28, 59	Citizens may file complaints with the ANPDP and appeal decisions.

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018) .

This table summarizes the main individual rights guaranteed by Law 18-07, emphasizing transparency, access, correction, and objection. These rights reflect the law's intent to give individuals control over their personal data and ensure legal remedies in case of abuse.

C. Obligations of Controllers and Processors

These articles define what organizations must do to comply with the law.

Table 10: Obligations of Controllers and Processors

Obligation	Articles	Summary
Security of processing	Art. 38	Controllers must implement appropriate technical and organizational measures.
Confidentiality and professional secrecy	Art. 40	Persons handling data are bound by professional secrecy.
Record keeping and traceability	Art. 41	Controllers must document their data processing activities.
Data minimization and retention	Art. 29–30	Only necessary data should be kept, and not longer than needed.
Contracts with processors	Art. 39	Controllers must ensure processors follow the law through binding contracts.

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018).

This table outlines the legal responsibilities assigned to data controllers and processors, from lawful processing to data security. It highlights the shared accountability required for protecting personal data throughout its lifecycle.

D. Cross-Border Transfers

These provisions regulate the flow of personal data beyond Algeria.

Table 11: Cross-Border Transfers in Law 18-07

Requirement	Articles	Explanation
General prohibition of transfers	Art. 42	Data transfer outside Algeria is prohibited unless certain conditions are met.
Adequate protection requirement	Art. 43	Transfers allowed only to countries with adequate data protection laws.

Authorizations by ANPDP	Art. 44–45	Transfers in special cases require prior approval from the authority.

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018).

The table presents the legal requirements for transferring personal data outside Algeria. It illustrates the law's restrictive approach to international transfers, requiring adequate protection levels or express authorization from the ANPDP.

E. Role of the Supervisory Authority (ANPDP)

The law defines how the ANPDP operates and enforces compliance.

Table 12: Role of the Supervisory Authority (ANPDP)

Function	Articles	Details
Investigative and oversight powers	Art. 49–51	ANPDP can conduct audits, access data, and issue orders.
Authorization and declarations	Art. 14–16	ANPDP receives declarations and grants authorizations for sensitive processing.
Issuance of guidelines and decisions	Art. 27–28	ANPDP can issue binding decisions and guidance for controllers.

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018).

This table details the institutional role of the ANPDP in enforcing Law 18-07. It showcases its regulatory, advisory, and sanctioning powers, which are essential for ensuring compliance and public trust in data processing activities.

F. Sanctions and Legal Remedies

This last thematic group details enforcement tools and legal consequences.

Table 13: Sanctions and Legal Remedies of the Law 18-07

Mechanism	Articles	Summary
Administrative sanctions	Art. 60–63	Includes warnings, suspension, and fines.
Criminal penalties	Art. 64–69	Covers unauthorized processing, data disclosure, or non-cooperation.
Judicial appeals and remedies	Art. 70–74	Individuals can challenge sanctions or request court review.

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018).

The table outlines the types of sanctions (administrative and criminal) for non-compliance. It illustrates the legal system's capacity to deter unlawful processing and compensate affected individuals.

3. Interdependence Between Protection and Processing in Law 18-07

Law No. 18-07 is built on the premise that personal data protection and the processing of such data are not distinct legal elements but are structurally integrated. The law imposes a set of data protection principles that apply directly to all stages of processing, making it impossible to process data lawfully without simultaneously implementing protection measures. This section explores how Law 18-07 constructs that interdependence, from the legal foundation of data processing to the way protection is embedded across the data lifecycle.

3.1. Processing as the Trigger for Protection Obligations

Under Law 18-07, personal data processing is considered a legally significant activity. It cannot be conducted unless it complies with specific protection standards. Articles 4 to 6 of the law establish core data protection principles, including lawfulness, transparency, purpose

limitation, data minimization, and proportionality. These principles are not optional ethical guidelines but legal conditions for valid data processing.

For example, Article 7 states that data processing must rely on one of several lawful bases, including the data subject's consent, a contractual necessity, a legal obligation, or the public interest. Article 13 outlines the strict conditions under which consent can be considered valid. Without meeting one of these legal bases, any processing is considered unlawful. Thus, the act of processing is not legally neutral; it is tightly regulated and must be justified according to the protection principles outlined in the law (République Algérienne Démocratique et Populaire, 2018, p. Article 7).

3.2. Enforcement of Protection Principles Through Operational Rules

Law 18-07 does not stop at declaring protection principles. It enforces them by assigning operational obligations to data controllers and processors. Each principle is translated into a legal rule that applies to specific stages or aspects of data processing.

Table 14: Protection Principles Through Operational Rules.

Protection Principle	Operational Rule (Processing Obligation)	Article(s)
Lawfulness	Legal basis required for processing	Articles 7–10
Transparency	Obligation to inform data subjects	Articles 17, 32
Purpose Limitation	Data used only for declared, legitimate purposes	Article 5
Data Minimization	Only necessary and relevant data may be collected	Articles 6, 30
Integrity & Confidentiality	Security and confidentiality measures must be implemented	Articles 38, 40
Accountability	Documentation and traceability of processing activities	Article 41
Data Subject Rights	Rights to access, rectification, opposition, and deletion	Articles 34–36

Source : Author's elaboration based on (République Algérienne Démocratique et Populaire, 2018).

This alignment ensures that protection is not merely a value declared in law, but an operational reality that governs daily data handling.

3.3. Lifecycle-Based Regulation: Protection at Every Stage

Another key feature of Law 18-07 is its lifecycle approach to personal data processing. From collection to erasure, each phase of the data lifecycle is subject to protection requirements:

- **Collection**: Requires a clear purpose and legal basis (Articles 5, 7–10), and users must be informed (Article 17).
- **Storage**: Must comply with security standards (Article 38) and be limited in time and purpose (Article 30).
- **Use**: Must remain consistent with the original declared purpose (Article 5); unauthorized uses are prohibited.
- **Sharing & Transfer**: Transfers to third parties or abroad are subject to prior authorization and must meet adequacy standards (Articles 42–45).
- **Deletion**: Once the purpose is fulfilled or upon user request, data must be erased unless a legal exception applies (Article 36), (République Algérienne Démocratique et Populaire, 2018).

This lifecycle logic ensures that protection is not static. Instead, it evolves in parallel with the flow of data, making protection a living, enforceable obligation throughout the processing chain.

3.4. Structural Integration: A Unified Legal Logic

The legal logic of Law 18-07 is based on integration rather than separation. Protection is not something external to processing or something that comes after—it is built into the very structure of what makes processing lawful. The existence of detailed obligations, enforced through the powers of the ANPDP, shows that protection is a precondition, a procedural framework, and an enforcement tool all at once.

For instance, the ANPDP is responsible for authorizing sensitive processing (Article 19), auditing compliance (Articles 49–51), and issuing administrative sanctions (Articles 60–63).

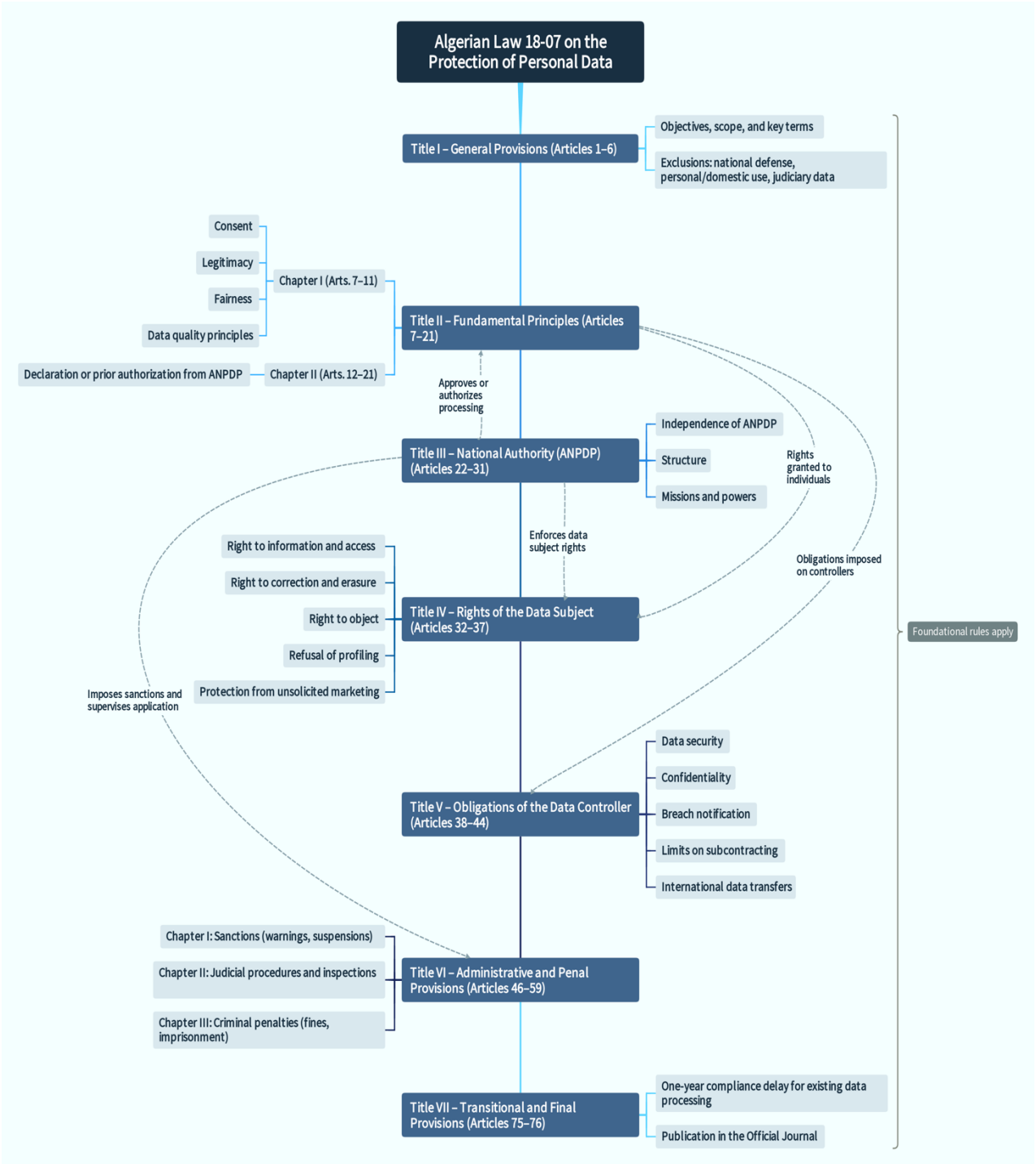
This shows that the implementation of protection principles is not left to voluntary interpretation but is monitored and sanctioned by institutional authority.

Law 18-07 offers a model in which the protection of personal data is activated, enforced, and maintained through the regulation of each processing operation. The law builds a system where processing is only legal if it respects protection**,** and protection is only meaningful when it shapes how data is processed. This interdependence reflects a comprehensive and modern legal logic, ensuring that data subjects' rights are preserved not in theory, but through enforceable practice (République Algérienne Démocratique et Populaire, 2018).

4. Visual Mapping of Law 18-07: Structure, Logic, and Enforcement Flow

This section provides a structured visual mapping of Law No. 18-07, highlighting its legal architecture, key principles, institutional mechanisms, and the rights and responsibilities it establishes. Through diagrams and synthesized models, the aim is to clarify the internal logic of the law and illustrate how its articles translate into operational obligations for data controllers, rights for individuals, and supervisory powers for the national authority.

Figure 9: Architecture of Law 18-07 - Titles and Structure

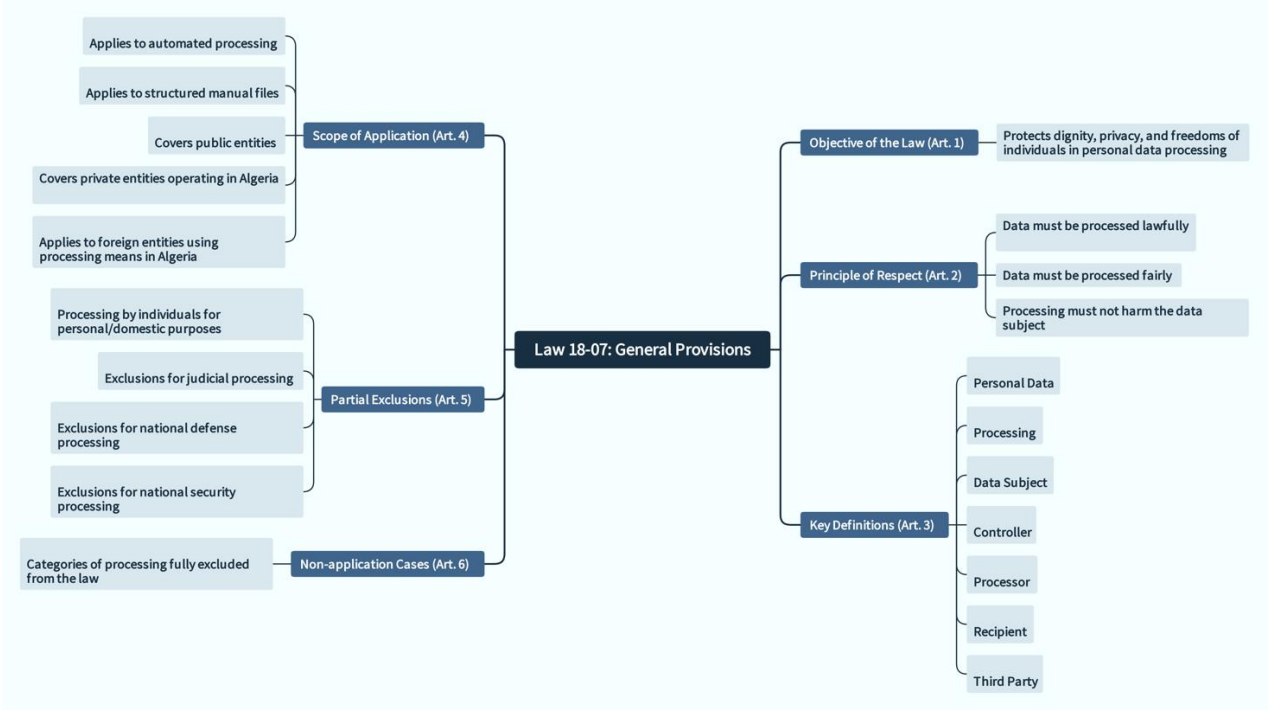


Source : Designed by the author, based on the official text of Law 18-07.

Chapter 1 : Theoretical Foundations and Conceptual Framework of Personal Data Protection

This chart outlines the structure of Law No. 18-07, which is divided into seven titles, each addressing a key dimension of personal data protection. It gives a macro-level overview of the law's architecture, helping to visualize the sequencing of general principles, rights, obligations, oversight, and sanctions.

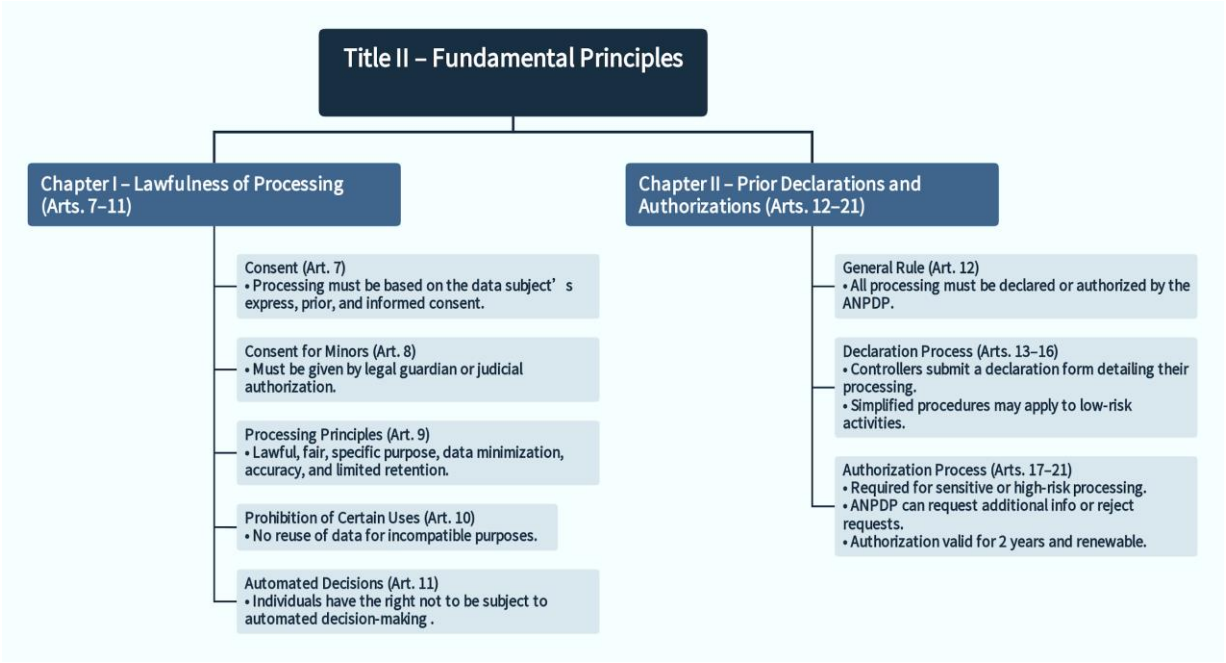
Figure 10: General Scope and Terminology of the Law.



Source : Designed by the author, based on Law 18-07, Articles 1–6.

This diagram presents the foundational definitions and general scope of the law, including what constitutes personal data, sensitive data, and the roles of data subjects and controllers. These terms set the groundwork for interpreting the rest of the legal text.

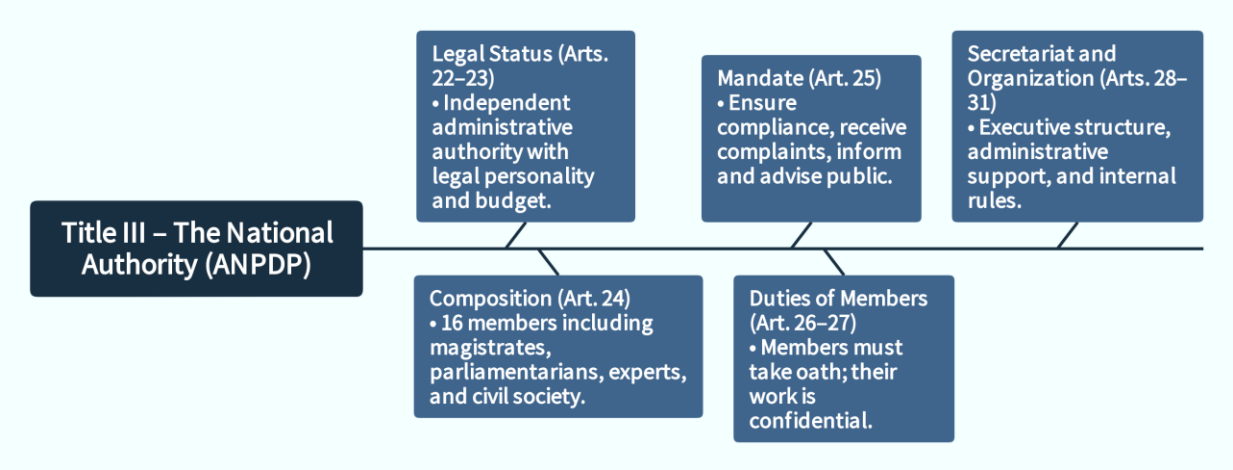
Figure 11: Lawful Bases for Data Processing under Law 18-07



Source : Designed by the author, based on Articles 7–21 of Law 18-07.

This graphic identifies the six legal grounds upon which data processing can be justified under Algerian law: consent, legal obligation, contract, public interest, vital interest, and legitimate interest. It mirrors the GDPR while maintaining national specificity.

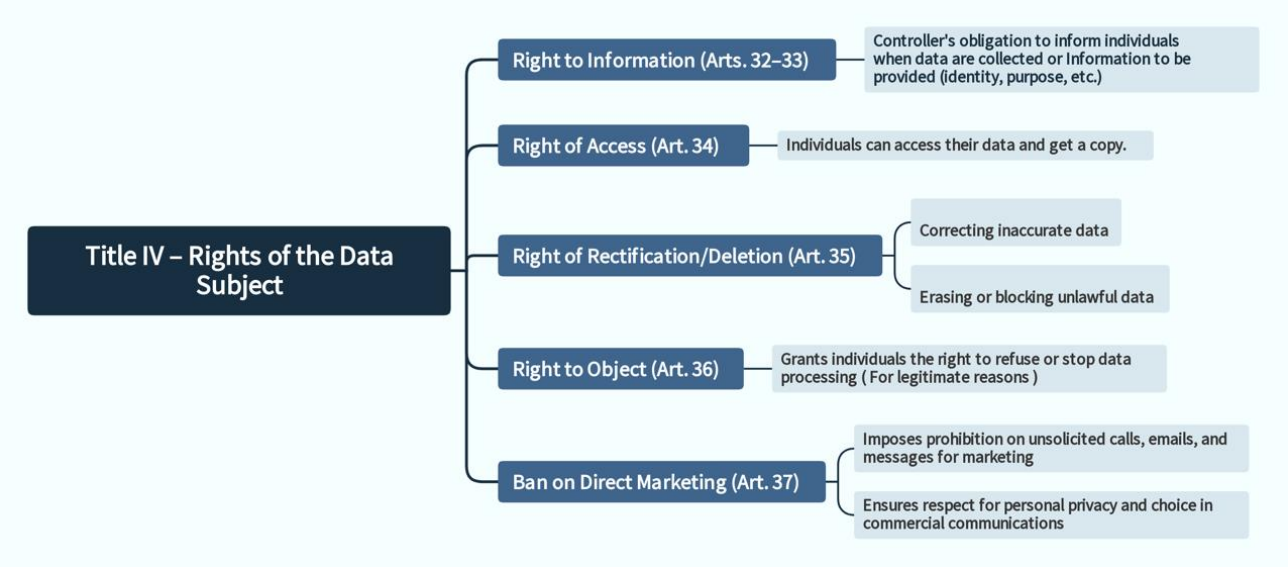
Figure 12: Institutional Role of the ANPDP



Source : Based on Articles 22-31, interpreted and designed by the author .

This chart outlines the functions of the national authority (ANPDP), including authorization, monitoring, audits, and the promotion of best practices. It shows how institutional enforcement is embedded in the law.

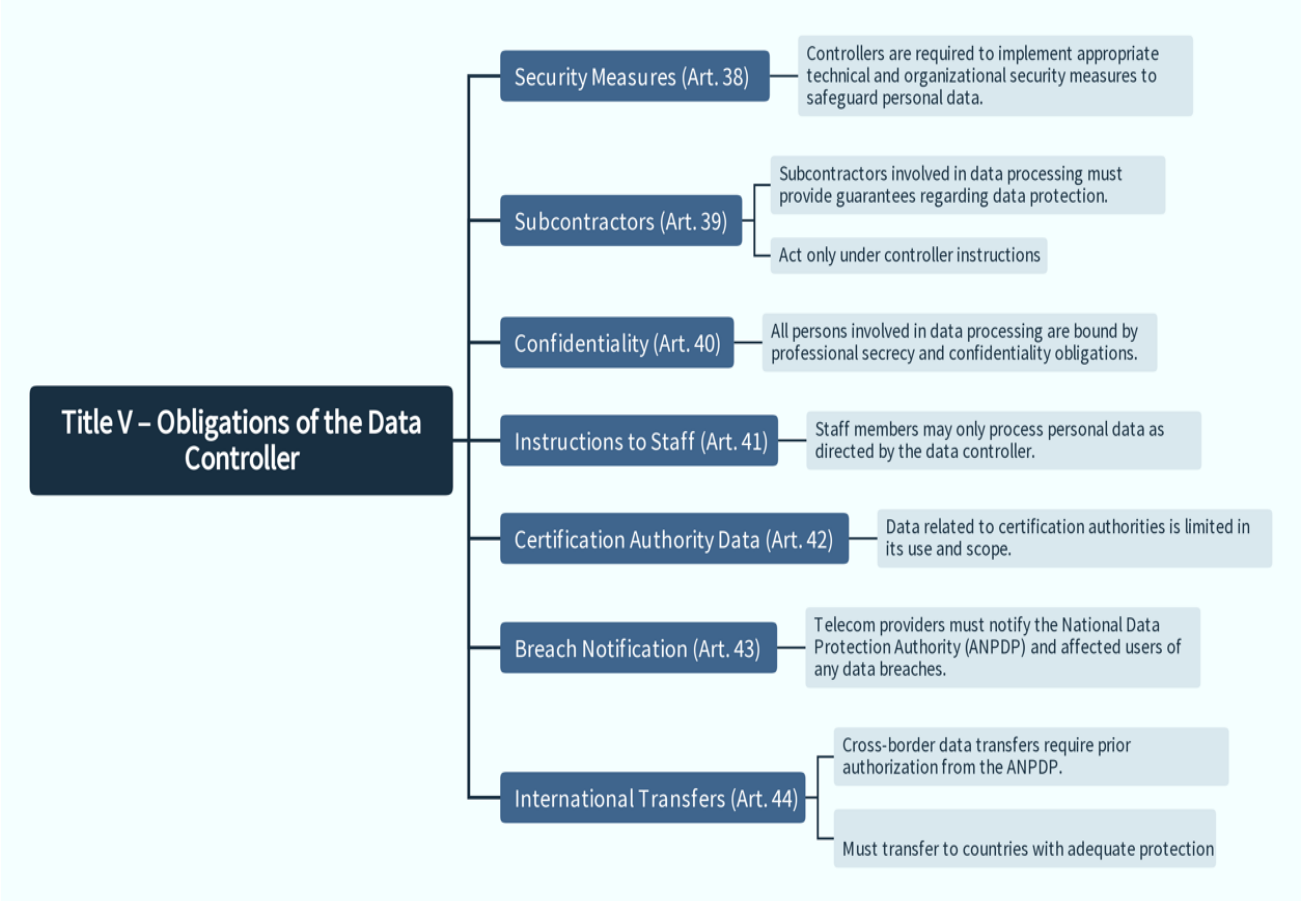
Figure 13: Rights of Data Subjects under Law 18-07



Source : Designed by the author, based on Articles 32–37 .

This figure highlights individual rights guaranteed by Law 18-07, such as access, rectification, deletion, and objection. It emphasizes the law's intention to empower individuals in the control of their personal information.

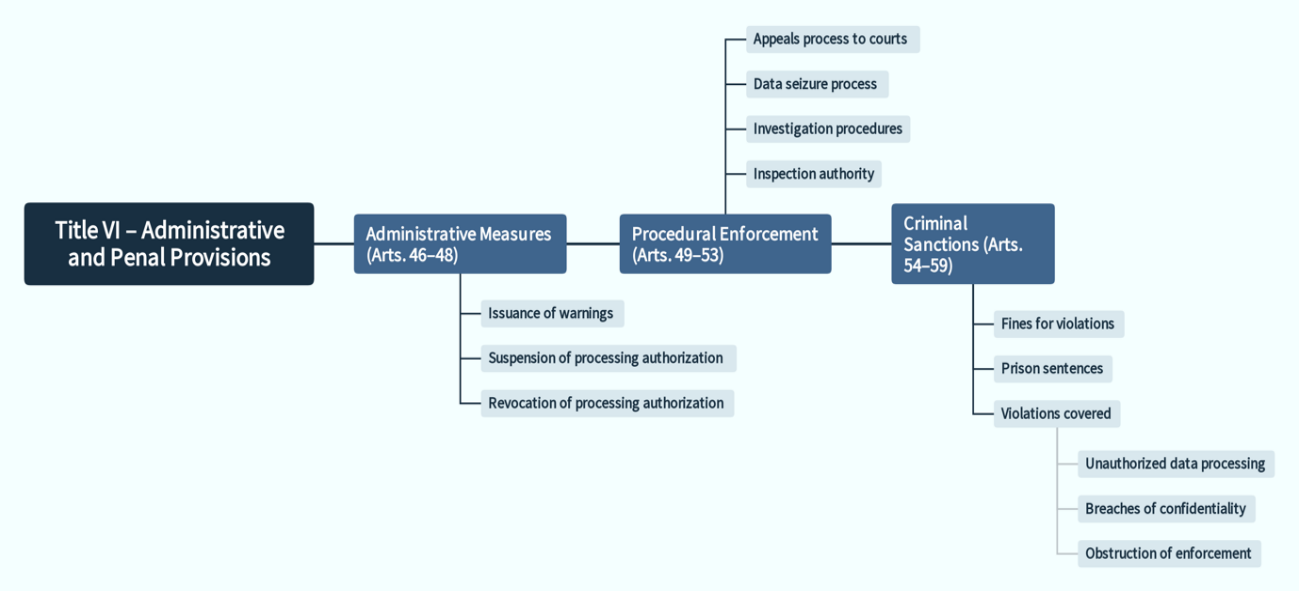
Figure 14: Obligations of the Data Controller under Law 18-07



Source : Designed by the author, based on Articles 38 –44 of Law 18-07

This diagram illustrates the core legal obligations imposed on the data controller, including the duty to ensure lawful processing, obtain explicit consent, secure sensitive data, maintain a register of processing activities, and cooperate with the ANPDP. These responsibilities form the operational backbone of compliance with the law.

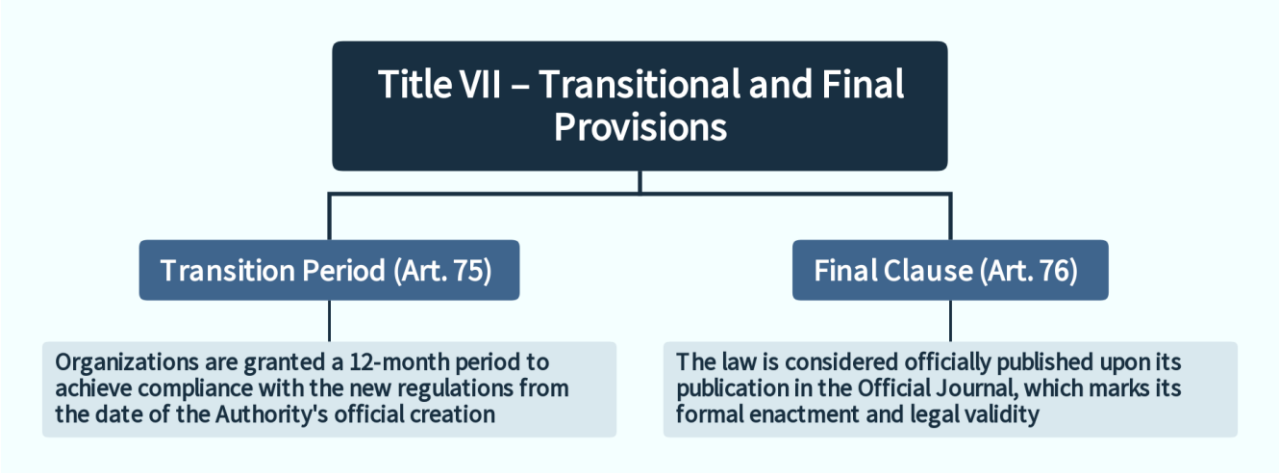
Figure 15: Sanctions and Enforcement Measures.



Source : Based on Articles 46 –59 of Law 18-07, visualized by the author

This visual summarizes the penalties (administrative and criminal) for non-compliance with the law. It also maps the types of infractions that trigger sanctions, reinforcing the law's seriousness and enforceability.

Figure 16: Transitional and final provisions



Source : Author's elaboration based on the Law 18-07, Articles 75-76 .

In summary, the cartographic analysis of Law 18-07 reveals a coherent and comprehensive legal framework inspired by international standards, yet tailored to Algeria's institutional context. Each figure highlights how the law distributes responsibilities, protects personal data, and ensures enforcement. This visual breakdown complements the textual analysis by providing an accessible and systematic overview of a complex legal instrument, helping organizations and researchers alike better understand its practical application.

This mapping concludes the theoretical foundation, preparing the ground for the practical case analysis to follow.

Conclusion

This chapter has established a comprehensive theoretical and legal framework necessary for critically engaging with the topic of personal data protection. By exploring the global challenges associated with data exploitation, the evolution of international regulatory instruments, and the ethical dimensions of information governance, it has highlighted the growing complexity of managing personal data in the digital age. The articulation of key terms and distinctions—such as between data controllers and processors, or anonymisation and pseudonymisation—has clarified the language through which legal responsibilities and data subject rights are defined.

Moreover, the analysis of foundational principles in instruments like the GDPR and ISO/IEC 27701 has demonstrated that data protection is not only a matter of compliance but also a matter of institutional trust, strategic positioning, and public accountability. The comparison with Algeria's Law 18-07 has revealed notable efforts to align with international standards, while also pointing to areas where legal definitions, operational mechanisms, and supervisory structures remain underdeveloped or require more robust implementation.

The cartographic mapping of Law 18-07 has made it possible to visualize the law's internal architecture, translating its abstract legal articles into an actionable model of rights, obligations, and enforcement. This provides an important bridge between theory and practice—illustrating how national legislation can be understood, interpreted, and applied in institutional contexts.

Having laid this foundational groundwork, the research now turns to the practical component of the study, where the goal will be to examine how these theoretical principles and legal requirements are operationalized in a specific organizational case. This transition from abstract norms to applied realities is essential for understanding not only what the law says, but how it functions in practice.

Chapter 2 : Compliance with Law 18-07: Case Study and Practical Insights

Introduction

To respond to the problem statement raised in this thesis, this practical part aims to apply the legal principles of personal data protection under Law 18-07 within a real organizational context. The objective is to evaluate the level of compliance and identify the key actions needed to ensure proper implementation of the law. Through a case study conducted within the company Cevital, we present the context of data processing, define the scope of the compliance project, and analyze the practices of a specific department—in this case, the Human Resources department. This part provides concrete insights into the challenges and opportunities of applying data protection regulations in a professional environment.

Section 1 : Company Overview and Data Processing Context

1. Overview of Cevital

Cevital is a major Algerian family-owned industrial group, founded in 1998 by Mr. Issad Rebrab. It was the first private company in Algeria to invest in such a wide range of sectors, including agri-food, electronics, household appliances, steel, flat glass, industrial construction, automotive, services, and media. Over the years, Cevital has evolved into one of the country's largest employers and a key driver of economic development.

The group employs more than 18,000 people across three continents, operating through 26 subsidiaries, and has positioned itself as a model of industrial diversification and international expansion. Its founder, Issad Rebrab, is known for his strong industrial vision and ambition to transform Algeria into a major exporting and emerging economy. The governance of the group is managed by a Board of Directors composed of his family members and independent advisors. The current CEO is Malik Rebrab.

Cevital's development strategy is based on several pillars: investment in high value-added sectors, continuous reinvestment of capital, adoption of advanced technologies, support for talent development, and a firm commitment to innovation and quality. The group aims to become a globally competitive industrial player, especially in export-oriented production (Cevital).

Cevital holds leading market positions in Algeria:

- No. 1 in sugar (90% market share)
- No. 1 in cooking oil (62%)
- No. 1 in flat glass (85%)
- No. 1 in food retail and white goods (washing machines, refrigerators)
- No. 1 non-hydrocarbon exporter
- No. 1 private contributor to the national budget

Its activities are structured into three main poles:

- Agri-food and Distribution**:** Cevital Agro-Industrie (based in Béjaïa) is the leader in food production and exports sugar, oil, and beverages to over 40 countries.

Figure 17: Agri-food and Distribution company branches

Source : (Cevital)

- Automotive, Real Estate, and Services: This pole includes vehicle distribution (Hyundai, Fiat, Alfa Romeo), car rental, real estate development, logistics, and advertising. New subsidiaries are being developed for vehicle assembly.

Figure 18: Automotive, Real Estate, and Services company branches

Source : (Cevital)

- Industrial Pole: Manages key subsidiaries such as Brandt (appliances), Oxxo (construction materials), MFG (flat glass), and NUMILOG (logistics), all of which support Cevital's industrial expansion in Africa and Europe.

Figure 19: Industrial Pole of cevital

Source : (Cevital)

2. Presentation of Cevital's Headquarters and Key Departments

2.1. Structure and Organization of the Headquarters

Cevital's corporate headquarters is located in Kouba, Algiers. It serves as the central hub for strategic coordination and administrative management for all of the group's subsidiaries. The organizational model at the headquarters is designed to ensure efficiency, compliance, and alignment with the group's overall objectives. Its structure mobilizes human, material, and financial resources to support decision-making and operational execution across Cevital's diverse business units (Cevital, 2024)

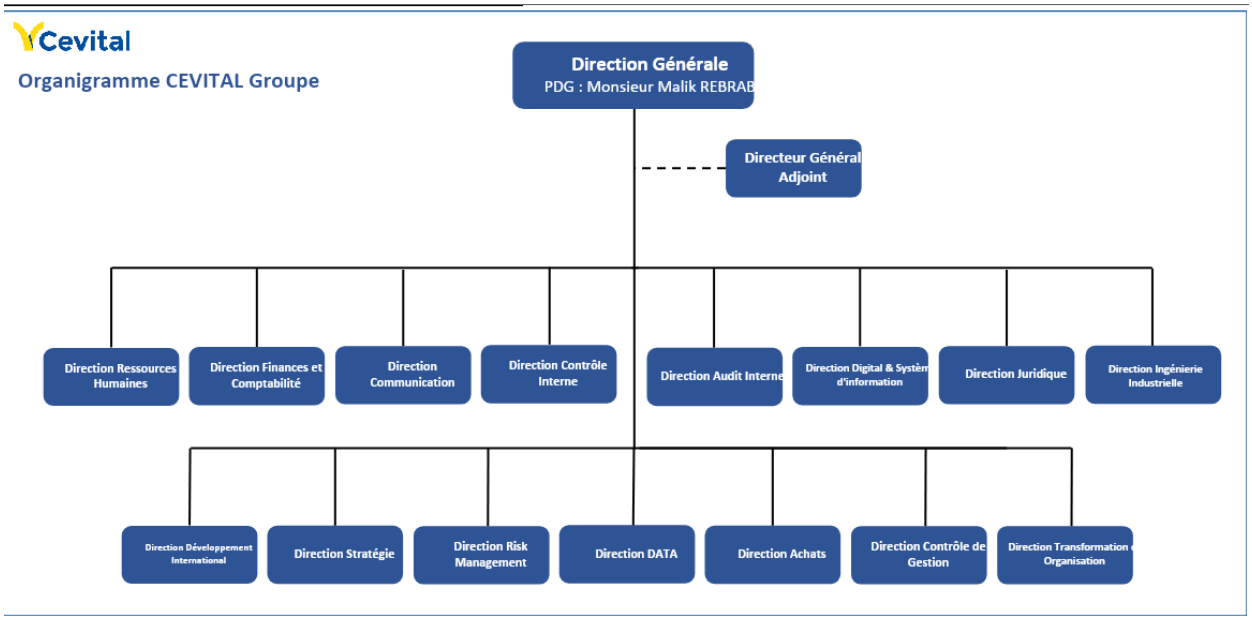
The General Management is supported by an Executive Secretariat and is composed of **15 core** directorates, each with a distinct role in managing critical aspects of the company's value chain. These include:

1. Marketing Directorate
2. Sales and Commercial Directorate
3. Finance and Accounting Directorate
4. Industrial Operations Directorate
5. Procurement Directorate
6. Logistics Directorate
7. Silos Operations Directorate
8. Beverages Directorate
9. Fats and Oils Directorate
10. Sugar Business Unit Directorate
11. QHSE Directorate (Quality, Health, Safety, Environment)
12. Energy and Utilities Directorate
13. Maintenance and New Works Directorate
14. Information Systems Directorate (DSI)

15. Human Resources Directorate

These directorates operate in an integrated manner, facilitating cross-functional coordination, policy implementation, and project execution. The responsibilities of two of these departments — the DSI and HR Directorate — are particularly critical in the context of digital governance and compliance with personal data protection laws (Cevital, 2024).

Figure 20: Organizational chart of Cevital headquarters



Source : (Cevital, 2024)

2.2 Information Systems Directorate (DSI)

The Information Systems Directorate plays a strategic role in supporting Cevital's digital infrastructure. Its mission is to develop, deploy, and secure the information technologies required to improve the performance, efficiency, and innovation capacity of the group.

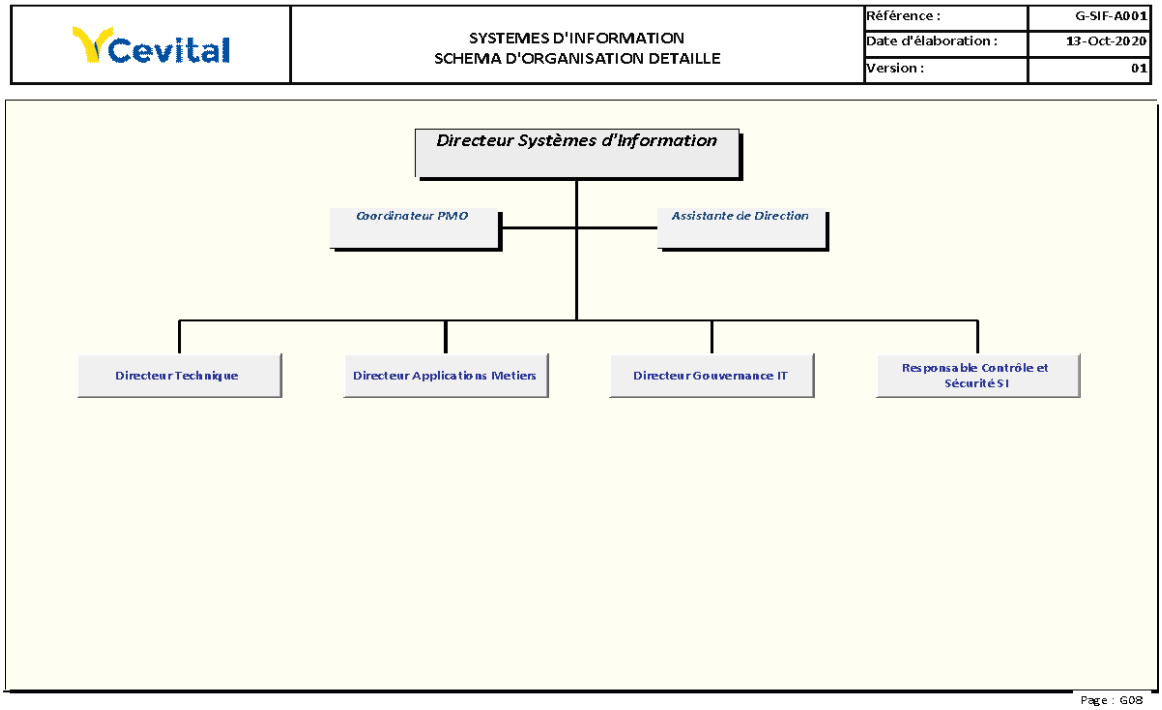
Key responsibilities of the DSI include:

- Planning and implementing IT solutions aligned with business strategy
- Developing internal platforms (e.g., SharePoint) and automating workflows
- Managing access control, system security, and data backup
- Ensuring the reliability and performance of the company's digital infrastructure

- Supporting compliance with IT security regulations and data protection laws

During the compliance project with Law 18-07, the DSI collaborated closely with the Human Resources and Legal departments. It played a critical role in designing tools for the inventory and mapping of personal data processing, and in ensuring the integrity and security of internal information flows (Cevital, 2024).

Figure 21: Organizational chart of the Information Systems Directorate



Source : (Cevital, 2024).

2.3 Human Resources Directorate (HR)

The Human Resources Directorate is responsible for designing and implementing human resource management policies that support the company's strategic objectives. It ensures that HR practices are aligned with Cevital group policies and adapted to operational realities.

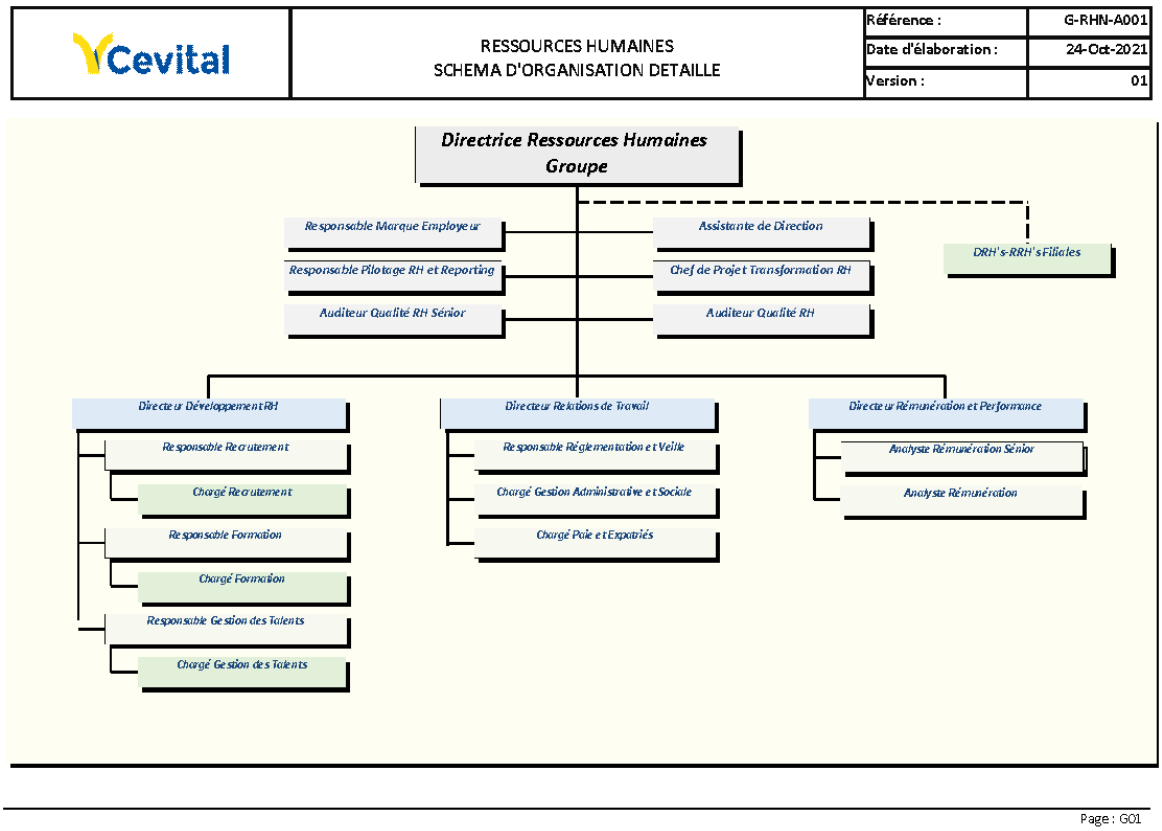
The HR Directorate performs a wide range of functions, including:

- Providing high-quality administrative support to all Cevital employees
- Leading recruitment, staffing, and career development programs

- Managing performance evaluations, compensation, and internal mobility
- Supporting disciplinary procedures and ensuring legal compliance
- Identifying training needs and developing employee skills
- Assisting general management and department heads in all HR-related matters
- Participating in the development of the group's internal communication strategy to promote employee engagement and organizational cohesion (Cevital, 2024).

As a key actor in the personal data protection compliance process, the HR Directorate served as the pilot department for the first three phases of the compliance project. Given the volume and sensitivity of personal data it manages (contracts, health records, disciplinary files), the department was prioritized for initial data inventory, legal mapping, and internal coordination with ANPDP requirements.

Figure 22: Organizational chart of the Human Resources Directorate



Source : (Cevital, 2024)

3. Nature of Personal Data Processed by Cevital

Cevital processes several categories of personal data related to its employees, service providers, and job candidates. These include:

- Full identification details (name, birth date, national ID, address)
- Professional data (employee ID, department, job title, contract type)
- Financial and administrative data (salary, bank account number, tax number, CNAS or CASNOS affiliation)
- Sensitive data (health declarations, absences, disciplinary measures)
- Contact and access data (email address, phone number, badge logs)

These data are collected and stored using a mix of digital platforms (HR management software, Excel files, internal portals) and physical documents. They are handled by multiple actors across the company, including HR staff, IT administrators, and department managers.

Due to the complexity of these operations and the associated legal risks, Cevital recognized the necessity to adopt a structured, transparent, and compliant approach in line with the new Algerian data protection framework (Cevital, 2024).

4. Strategic Relevance of Compliance with Law 18-07

In response to the enactment of Law 18-07, Cevital launched a structured initiative in 2024 to ensure full compliance with personal data protection obligations. The law requires organizations to declare data processing activities, uphold data subjects' rights, implement robust data security measures, and maintain transparency with the ANPDP .

The compliance project was structured into successive phases, including internal awareness efforts, data processing inventory and mapping, regulatory declarations, validation by the supervisory authority, and the integration of compliance tools and training programs. Early stages of the initiative focused on raising awareness among internal stakeholders, developing tools for identifying and categorizing processing operations, and preparing legal mappings—particularly within the HR domain.

These foundational efforts laid the groundwork for a broader organizational adaptation to the new regulatory environment and provided practical material for the analytical sections that follow in this thesis, which examine the challenges and operational implications of implementing Law 18-07 within a large enterprise (Cevital, 2024).

Section 2 : Context and Objectives of the Compliance Project

1. Project Context and Objective

In early 2024, in response to the enactment of Law 18-07 on the protection of personal data, the CEVITAL Group launched a strategic and high-priority compliance initiative. The project was developed as part of the Group's broader governance transformation efforts, aimed at strengthening legal risk management, enhancing information security, and embedding data protection principles into the company's operational culture.

Recognizing both the legal obligations and the reputational risks associated with non-compliance, CEVITAL adopted a proactive and structured approach to ensure that all personal data processing activities across the organization would be brought into full alignment with the new regulatory framework (Cevital, 2024).

The initiative was deployed at the headquarters level, under the joint supervision of the Legal Affairs Department, the Information Systems Department (DSI), and the Human Resources Department (DRH). However, the project extended far beyond HR alone — it involved all directions and departments handling personal data, including but not limited to:

- Procurement (Direction des Achats)
- General Resources (Direction des Moyens Généraux)
- IT and Information Systems (DSI)
- Internal Audit and Management Control
- Legal and Compliance Units

This enterprise-wide scope reflects the transversal nature of data protection and the company's commitment to institutionalizing compliance as a core function.

1.1. Objectives of the Project

The overarching goal of the project was to establish an operational and legally compliant framework for managing personal data processing within the organization. In line with the provisions of Law 18-07, this included:

- Identifying and documenting all data processing operations involving personal data,
- Declaring or requesting authorization for these operations through the ANPDP ,
- Ensuring the protection of data subjects' rights (access, rectification, objection, etc.),
- Implementing technical and organizational measures to guarantee confidentiality, integrity, and legality of processing.

The project also sought to assess the organization's level of readiness, to develop tools (legal and procedural), and to institutionalize a culture of compliance (Cevital, 2024).

1.2 Structuring of the Project

The compliance roadmap was organized into seven sequential phases, each aligned with the logical progression of data governance prescribed by Law 18-07

Phases	Explication
Phase 1: Awareness and Training	Educating internal stakeholders (managers, focal points, employees) on the legal framework, responsibilities, and importance of compliance.
Phase 2: Inventory of Data Processing Operations	Identifying all existing personal data processing activities across departments, using standardized templates based on ANPDP's official forms.
Phase 3: Mapping and Register Development	Structuring collected data into a legal mapping system and a compliance register to prepare for declaration.
Phase 4: Submission of Declarations	Declaring the identified processing activities through the ANPDP portal and requesting validation or authorization as needed.

Phase 5: Feedback and Adjustment Phase	Integrating the ANPDP's recommendations or compliance observations and modifying internal systems accordingly.
Phase 6: Implementation of Technical and Organizational Measures	Developing the internal tools (e.g., access controls, compliance procedures, documentation systems) necessary to support ongoing compliance.
Phase 7: Training and Rollout	Final deployment of procedures and tools across the company and continuous training for relevant staff.

1.3. Departmental Focus and Scope of Work

Although the compliance project encompassed all departments involved in personal data processing, the Human Resources Department (DRH) was selected as the lead unit for the implementation of the first three phases. This decision was based on several strategic and operational factors:

- The HR department handles the highest volume and most sensitive categories of personal data (e.g. identity, salary, health, social security),
- Its data processing operations span the full employee lifecycle (recruitment, contract management, training, evaluation),
- It serves as a model for data governance due to its internal transversal function.

Accordingly, the first phases of inventory, mapping, and preliminary compliance analysis were concentrated within the HR domain, providing a representative foundation for later generalization across the organization.

This thesis focuses specifically on these first three phases, with particular attention to the analysis and mapping of personal data processing as both a legal obligation and a strategic compliance instrument under Law 18-07.

2. Focused Implementation Stages within the Framework of Compliance with Law 18-07

2.1. Step 1: Awareness and Engagement

2.2.1. Objective and Strategic Importance

The first phase of Cevital's compliance project with Law 18-07 was dedicated to raising awareness and engaging internal stakeholders. This step was essential to ensure a shared understanding of the new legal requirements and to build a compliance culture aligned with the regulatory expectations set forth by the ANPDP.

Law 18-07, particularly Articles 4 through 6, establishes the principles of accountability, legality, and transparency in data processing. It also assigns responsibility to organizations for guaranteeing that all processing activities respect individuals' rights and are conducted under clearly defined legal grounds. Consequently, internal alignment and stakeholder sensitization were necessary to prepare departments to contribute actively to the following stages of the compliance process.

The strategic objectives of this first phase included:

• Disseminating the core principles and obligations of Law 18-07,
• Clarifying the roles and responsibilities of department heads and data focal points,
• Establishing an internal compliance vocabulary that could be shared across functions,
• Creating foundational materials to support regulatory understanding.

This phase formed the institutional foundation for the practical execution of the project's next stages.

2.1.2 Methodology and Tools Used

To initiate the compliance project, a qualitative and collaborative methodology was adopted, combining regulatory analysis with operational adaptability. The approach relied on awareness-raising, legal clarification, and the development of customized internal tools suited to the organizational context of Cevital.

❖ **Stakeholder Engagement and Awareness Strategy**

Workshops and sensitization meetings were conducted with focal points and department heads from HR, IT, Legal, and Logistics. These sessions introduced the objectives of the compliance program, explained the seven project phases, and outlined the requirements of Law 18-07. The official project presentation was used to provide a clear framework, while additional support materials—including a bilingual project brief and posters—were distributed to ensure continuity beyond the meetings (Cevital, 2024).

❖ **Semi-Structured Interview with the ANPDP**

To address legal ambiguities and align internal practices with regulatory expectations, a semi-directive interview guide was developed and submitted to the ANPDP. The guide, divided into six thematic parts, aimed to clarify the following:

1. **Présentation de l'ANPDP**: Mission, governance, and operational scope of the authority.
2. **Conformité Légale et Pratiques**: Procedures for declaration vs. authorization, and handling of cross-border transfers.
3. **Communication et Soutien**: ANPDP's methods for enterprise support, including training and documentation.
4. **Rôle et Responsabilités**: Definition of the DPO role and internal audit practices.
5. **Innovations et Perspectives**: Use of ICT, data security technologies, and expected legislative developments.
6. **Suggestions d'Amélioration**: Feedback mechanisms between enterprises and the regulator. (Cevital, 2024)

The responses were documented in a formal report (Appendix A – Legal Interview Guide and Summary Report), which became a reference for later project phases, particularly legal mapping.

❖ **Educational and Legal Tools Developed**

A set of tailored tools was created to facilitate understanding, standardize practices, and reinforce internal accountability:

A. Security and Personal Data Protection Charter

A bilingual charter (French and Arabic) was drafted and approved by the Legal Affairs Department. It outlines:

- Definitions of personal data and key roles (controller, processor),
- Employee responsibilities for data confidentiality, secure handling, and access control,
- Best practices in digital and physical data management,
- Disciplinary measures for breaches of policy.
  This charter was distributed during onboarding and compliance meetings (Appendix B).

B. Awareness Poster on Law 18-07

Designed for maximum visibility, the bilingual poster communicates:

- Fundamental principles (lawfulness, minimization, purpose limitation),
- Core rights of data subjects (access, rectification, objection),
- Operational best practices for secure and compliant data handling.
  It was posted in communal areas and disseminated via internal communication channels (Appendix C).

2.1.3 Institutional Impact and Alignment

This first step established the foundations of legal compliance at the organizational level. It enabled Cevital to:

• Ensure that the compliance process was not perceived as a purely legal formality, but rather as an integral part of operational governance,

• Align internal language and understanding around Law 18-07,

• Clarify expectations for department managers and data focal points,

• Secure regulatory guidance from the ANPDP to avoid misinterpretation in subsequent phases.

The tools produced during this phase were later integrated into the broader compliance framework and served as references for communication, legal validation, and internal training. All materials cited are included in their full version in the appendices.

2.2. Step 2: Inventory of Personal Data Processing

2.2.1 Objective and Legal Context

The second phase of the compliance project focused on the identification and documentation of all personal data processing operations within the organization. In accordance with Articles 29 to 31 of Law 18-07, data controllers are required to maintain a complete record of data processing activities under their responsibility. This record must include information related to the purpose of processing, the categories of data and data subjects, the legal basis, the retention period, and the recipients of the data.

The objective of this phase was therefore to establish an accurate and standardized inventory of processing activities, starting with the Human Resources department, chosen as the pilot unit due to the volume and sensitivity of the data it manages.

2.2.2 Methodology Adopted

The methodology followed during this step was based on:

- A preliminary analysis of the official forms provided by the ANPDP for declaring processing operations,
- A simulation of these forms to test their applicability to internal practices,
- The design and deployment of an internal digital platform (SharePoint) that enabled focal points from various departments to input their processing operations in a structured manner.

The approach prioritized replicability**,** legal accuracy, and ease of use, in order to encourage participation from departments unfamiliar with legal terminology or data governance procedures.

2.2.3 Simulation of the ANPDP Declaration forms

The ANPDP provides 11 official form types to be used for declaring personal data processing operations, depending on the nature and purpose of the data involved. These include forms for human resources, video surveillance, client data, health-related data, and others (Appendix D).

To facilitate the internal inventory, these forms were digitally reproduced in Excel format**,** simulating each data entry field and validation step present in the official versions. These simulations allowed for:

- Testing the relevance of each form to actual internal processing cases,
- Identifying points of overlap, redundancy, or missing categories,
- Standardizing the way data processing activities were described across departments.

Each simulation included sections for:

- The identity and contact information of the data controller,
- Description of the processing purpose,
- Legal basis under Law 18-07,
- Categories of data and data subjects,
- Means of collection and transmission,
- Recipients of the data,
- Data retention periods,
- Security measures applied.

These templates served as preparatory forms before any submission to the ANPDP portal.

2.2.4 Creation of the Internal Collection Platform (SharePoint)

Following the simulation phase, the digitized forms were integrated into a custom SharePoint platform developed with support from the DSI. The platform allowed for:

- Secure online access by department focal points,
- Real-time entry and saving of data processing records,
- Centralization of all inventory data for validation and future declaration,
- Compatibility with the ANPDP's submission requirements.

The SharePoint system was designed with form validation controls**,** dropdown menus, and pre-filled legal references to reduce errors and ensure consistency. It functioned as both a data collection tool and a preliminary registry model (Appendix E).

Internal communications and brief training sessions were conducted to assist focal points in understanding how to use the platform and fill out their department's processing activities accurately.

2.2.5 Inventory Results – HR Department Focus

The Human Resources department was selected as the lead scope for this phase. Through the platform and simulated forms, 15 personal data processing operations were identified and documented. These included:

• Employee recruitment and onboarding (including CV collection and candidate processing),

• Management of apprentices and interns,

• Payroll management and salary payments,

• Social security declarations (CNAS, CASNOS),

• Health insurance and mutual fund management,

• Occupational health and medical surveillance,

• Leave and absence management,

• Training management and employee development tracking,

• Performance evaluations and career development,

• Disciplinary procedures and incident management,

• Access control and badge tracking,

• Internal HR reporting and dashboards,

• Salary review and compensation adjustments,

• Employer branding campaigns and communication (e.g., LinkedIn),

• Internal newsletters and communication distribution.

Each processing operation was described using a consistent framework based on the legal requirements of Law 18-07, including purpose, legal basis, actors involved, data flows, retention period, and security controls (Cevital, 2024).

The data collected during this step constituted the core material for the mapping and register development phase.

2.3. Step 3: Analysis and Mapping of Processing Activities

2.3.1 Objective and Regulatory Foundation

The third phase of the compliance project aimed to create a structured cartography (mapping) and processing register of the personal data operations identified during the inventory stage. This effort is grounded in the requirements of Articles 29 to 35 of Law 18-07, which obligate data controllers to maintain a comprehensive internal record of all personal data processing activities.

These records must be:

- Transparent and legally documented,
- Aligned with declared or authorized activities,
- Readily available for submission to the National Authority for the Protection of Personal Data (ANPDP) upon request, and
- Adaptable to evolving operations or regulatory audits.

This phase plays a pivotal role in establishing a sustainable and auditable data protection framework, as it allows organizations to:

- Understand and visualize personal data flows across internal systems,
- Identify gaps**,** legal risks, or areas of non-compliance**,**
- Facilitate ANPDP declarations through centralized and standardized documentation.

2.3.2 Methodological Framework for Legal Mapping of Processing Activities

This phase employed a methodology aimed at transforming raw inventory data into a structured, legally compliant representation of processing activities. The process unfolded in two main stages: (1) legal categorization and documentation of each processing operation, and (2) development of a visual flowchart depicting data movements.

The steps included:

- Categorizing the 15 processing activities by their legal purpose (e.g., administrative, legal obligation, contractual necessity) and their business function within HR processes (e.g., recruitment, payroll, training).
- Identifying involved actors, including internal roles (data controller, data processor) and external third parties (e.g., insurance providers, CNAS, CASNOS).
- Defining the legal basis for each operation in reference to Articles 7–10 of Law 18-07, distinguishing among consent, legal obligation, public interest, and contractual justification.
- Mapping internal and external data flows, retention periods, categories of data processed, and the technical and organizational security measures applied.
- Designing a visual flowchart illustrating the personal data lifecycle and interrelations between processes, facilitating clear understanding of data movements within and beyond the organization.

This approach prioritized:

- **Legal clarity:** ensuring all components complied with national regulations.
- **Operational realism:** respecting existing workflows and organizational systems.
- **Visual simplicity:** producing accessible cartography for non-specialist stakeholders.

2.3.3 Application of Legal Mapping to HR Department Processing Activities

Building on the methodological framework described in Section 2.3.2, a detailed legal mapping of the HR Department's 15 processing activities was constructed following the analytical dimensions recommended by the ANPDP:

- Name and objective of each processing operation.
- Categories of personal data involved.
- Legal basis for processing (consent, legal obligation, etc.).
- Actors involved (data controllers, processors, external recipients).
- Geographic scope of data flows, including any international transfers.
- Technical and organizational security safeguards implemented.

The mapping process was operationalized using internal documentation templates, SharePoint collaboration tools, and Excel registers developed during the inventory phase. The final visual flowchart, which represents the comprehensive data lifecycle and inter-process relationships, will be presented and analyzed in detail in Section 2.5.

Section 3 : Analysis and mapping of Processing Activities – HR Department

1. Analytical Objective

This section presents the analysis of the results obtained during the inventory phase of personal data processing operations within the Human Resources Department (DRH)**.** The objective is to evaluate the completeness**,** regulatory alignment, and compliance risks associated with the 15 HR processing activities identified. This analytical step serves as a bridge between data collection and legal mapping, enabling a deeper understanding of the data ecosystem before visualizing it through a compliance cartography.

The analysis focuses on key compliance indicators as defined by Law 18-07, including:

- Legal basis of processing,
- Nature and sensitivity of data collected,
- Retention practices,
- Data recipient categories,
- Internal versus external processing actors,
- Security and access management practices.

1.1. Overview of the Inventory Dataset

The dataset analyzed is the product of the internal census conducted within the DRH using a SharePoint platform and simulated ANPDP declaration forms. Each processing operation was described according to a standardized legal template that includes:

- Title and functional description of the processing,
- Categories of personal data used (identity, financial, health, etc.),
- Data subject groups (e.g. candidates, employees, interns),
- Legal purpose and justification (Articles 7–10 of Law 18-07),
- Means and tools used (Excel, HR software, physical archives),
- Retention periods,

- Type of processing (manual, automated, or hybrid),
- Data sharing with third parties,
- Security measures and responsible units.

1.2. Key Findings

A. Legal Basis Distribution

Among the 15 HR processing operations analyzed:

- 11 operations are based on legal or contractual obligations, such as payroll, social security declarations, occupational medicine, and apprenticeship management.
- 3 operations (e.g. performance evaluation, internal communications, employer branding) are based on legitimate interest and may require internal justification documents.
- 1 operation (CV collection and candidate databases) involves **consent**, especially for long-term retention beyond the recruitment cycle.

This distribution suggests that while most processing is justified by legal duties, procedures for consent and interest balancing tests should be reinforced for certain operations.

B. Sensitive Data Processing

At least 5 processing operations involve sensitive data under Article 10 of Law 18-07, including health-related data (justifications for absence, occupational medicine),

These require specific security measures and, in some cases, prior authorization from the ANPDP, depending on the data sensitivity and purpose.

C. Processing Means and Format

The majority of processes are carried out through hybrid systems, combining:

- Manual tools (Excel files, paper documents),
- Semi-automated systems (SharePoint, emails),

- Fully automated tools (payroll software, performance tracking platforms).

This highlights a need for clear documentation of access rights and audit trails, particularly for hybrid environments where data security risks are higher.

D. Data Retention Practices

Retention periods varied significantly:

- Some processes (e.g. payroll, tax declarations) follow legal durations (5–10 years),
- Other types of processing—such as those related to internal newsletters or employer branding—are subject to a fixed retention period of **20 years**, which may require further justification in light of the data minimization and storage limitation principles established by Law 18-07.

E. Internal and External Recipients

Most data remains internal to Cevital; however, several processes involve communication with:

- **Public institutions** (CNAS, CASNOS, tax administration),
- **Third-party service providers** (e.g. medical partners, training centers),
- **Digital platforms** (LinkedIn campaigns, HR analytics tools).

This underscores the importance of **contractual safeguards** (clauses, DPAs) with third parties and a tracking mechanism for international transfers, if applicable.

1.3. Categorization of Processing Activities

For greater operational clarity and to facilitate visual mapping, the 15 processing operations were categorized into five functional clusters, each aligned with a common legal and organizational purpose

Categories	Processing operations
1. Employee Lifecycle Management	- Apprenticeship management - Intern management - Collection and processing of CVs and applications - Reference verification (candidates) - Interview management - Personal administration
2. Compensation and Benefits	- Payroll processing - Health insurance management - Salary review
3. Training and Performance	- Training management - Performance management
4. Internal Communication and Employer Branding	- Internal Newsletters and Communications - Employer Branding campaigns (LinkedIn)
5. Health and Legal Interactions	- Occupational health

This classification allows for a clearer understanding of personal data flows across operational domains and supports targeted compliance efforts for each category.

1.4. Detailed Analysis Example – "Administration du Personnel"

To concretely illustrate the analysis approach, the processing operation "Administration du Personnel" is examined in detail. This process is at the core of HR management, involving the continuous handling of employee records throughout the employment lifecycle (Cevital, 2024).

Table 15: Form 1_General Processing Information

Field / Element	Processing 1
Name of the processing activity	Personnel Administration
Type of processing	Manual / Automated
Purpose of the processing	To structure, organize, and manage all activities related to personnel administration while ensuring compliance with legal and internal rules
Legal basis of processing	- Consent - Legal obligation - Contract execution
Focal point's title	Administrative Management Officer
Department	DRHG
Processing categories	- Personnel Management
Existence of subprocessors	Yes

Table 16: Form 2_Subprocessing Information

Field / Element	Processing 1
Subprocessing name	Time Tracking Management
Type of processing	Automated
Purpose	Efficient management of working hours
Outsourced?	no
Name and surname	/
Observations	/

Table 17: Form 3_Subcontractor Identity (Empty fields)

Field / Element	Processing 1
Legal/Natural person	/
Name / Company name	/
First name / Abbreviation	/
Adress	/
Country	/
City	/
Field of activity	/
Website	/
Existence of a signed contract with the subcontractor (contract compliant with Article 39 of Law 18-07)	/

Table 18: Form 4_Data Collection Methods

Field / Element	Processing 1
Data collection type	**Manual / Automated**
Collection methods	**- Intranet** **- Offline workstation** **- Paper**
Security measures for data collection	**- Traceability**
Categories of data subjects	**- Employees**
Other data sources used?	**Yes**
Name (DB or FM)	**SAP / Portail RH / CREDOID**
Owning department	**HR Department**
Collection means	**- Paper** **- External media** **- Connection**
Purpose	**Personnel management and time tracking**

Table 19: Form 5_Categories and Types of Data Collected

Field / Element	Processing 1

Categories of data	**- Personal data** **- Professional data** **- Sensitive data**
Types of data	**<u>Types of personal information:</u>** **- National ID number** **- Social security number** **- Name and surname** **- Date and place of birth** **- Marital status** **- Photo** **- Home address** **- Email address** **- Phone number** **- Spouse/Children name, birth date, place of birth** **- Military status** **- Driver's license** **- Degrees** **- Previous employer certificate** **- Criminal record** **- Passport number (for expatriates)**
	<u>Financial data :</u> **- Salary** **- Bank account** **- Remuneration elements (base salary, bonuses, tax)**
	<u>Sensitive data :</u> **- Biometric fingerprint** **- Blood type** **- Medical certificates** **- Serology (for expatriates)**
	<u>Professional data :</u> **- Employee ID** **- Hiring date** **- Department / Position** **- Supervisor** **- Departure date and reason** **- Attendance data** **- Professional phone and email**
Data origin	**- Concerned person** **- Other**

Data sources	**- Forms** **- Paper files** **- Databases**
Retention duration	**Limited**
Specify the duration?	**10 years after end of employment**

Table 20: Form 6_Data storage

Field / Element	Processing 1
How is the data stored?	**Manual / Computerized**

Table 21: Form 7_Manuel data storage

Field / Element	Processing 1
Name of the database	**SAP/SAGE/CREDOID/Portail RH/Excel**
Database storage location	**Server**
Legal framework	**Compliance with Law 18-07**
Name of the manual file	**Dossiers salariés**
Manual file storage location	**DRH**
Legal framework	**Compliance with Law 18-07**

Table 22: Form 8_Computerized data storage

Field / Element	Processing 1
Do you share personal data with third parties or have interconnections?	**Yes**
If yes	**Yes**
Name of the recipient organization	**CNAS / Impôts / Inspection du Travail / Direction de l'emploi**
Mode of communication	**- Papier** **- Connection**
Objectives	**Legal obligation**
Legal framework	**- Law No. 90-11 of April 21, 1990 on labor relations** **- Law No. 81-10 of July 11, 1981 on the conditions of employment of foreign workers**

Table 23: Form 9_Data transfer

Field / Element	Processing 1
Are the processed data transferred to another country?	**No**
If your processing involves a transfer of data abroad, please submit to the ANPDP the authorization request form **(In accordance with the provisions of Articles 25 point 5 and 44 of Law No. 18-07, any data controller who wishes to transfer personal data abroad is required to submit a request to the national authority).**	

Table 24: Form 10_Rights of the data subject

Field / Element	Processing 1
Is there consent from the data subjects?	**Yes**
If yes	
Indicate the method of consent	**Data Protection Notice / Employment Contract**

Table 25: Form 11_Declarations and Commitments Regarding Personal Data Processing

Choices / Options	Processing 1
I commit to carrying out the processing in accordance with the provisions of Law No. 07-18 of June 10, 2018, relating to the protection of natural persons with regard to the processing of personal data	**Yes**
I commit to promptly informing the DPO of any changes to the declared information as well as the termination of the processing.	**Yes**
I solemnly declare that the information covered by this declaration is truthful, complete, accurate, and complies with the requirements of the legislation on the protection of personal data.	**Yes**

Source : Author's own elaboration based on internal documents, (Cevital, 2024)

This example serves as a model for mapping in Section 2.6, as it represents a typical operation with legal, organizational, and technical complexity.

Based on the analysis, the following observations emerge:

- The HR department demonstrates a strong commitment to data protection, with structured operations and legal awareness.
- Gaps remain in areas like consent documentation, retention control, and hybrid access traceability.
- High-risk operations involving sensitive data (e.g. health, evaluation, or disciplinary files) require reinforced safeguards.

These findings directly inform the legal mapping strategy and will be visualized and interpreted in the next section.

2. Legal Mapping and Visual Cartography of HR Processing Activities

2.1.Objective of the Mapping

Following the analytical assessment of the 15 personal data processing operations conducted within the Human Resources Department, this section presents a structured visual mapping (cartographie) of these operations in alignment with the compliance requirements of Law 18-07**.**

The objective of this cartography is to:

- Represent the functional and structural organization of personal data flows in the HR department,
- Illustrate the relationship between processing categories and specific operations,
- Highlight compliance responsibilities, actors, and legal justifications in a visual and accessible format,
- Serve as a practical support for internal governance, ANPDP declarations, and future audits.

This cartographic exercise also supports Article 31 of Law 18-07, which requires data controllers to maintain a structured and transparent register of processing operations.

2.2. Methodology of Construction

The cartography is based on the data inventory, legal qualification, and classification conducted during the analysis phase. The construction of the map follows a layered and hierarchical logic, structured as follows:

- **Central Node**: Personal data processing in the HR department (compliance object),
- **First Layer**: Functional categories of processing (e.g. recruitment, payroll, health),
- **Second Layer**: The 15 processing operations identified during the recensement,
- **Third Layer (Focused Detail)**: In-depth mapping of a representative operation — Administration du Personnel — including legal basis, data types, actors, and security mechanisms.

This approach combines legal structure, functional clarity, and visual simplicity, ensuring that the map is intelligible for both legal stakeholders and operational managers.

2.3. Selected Mapping Focus – Administration du Personnel

To avoid excessive visual density and facilitate interpretation, only one processing operation — "Administration du Personnel" — is represented in full detail in this cartography. This operation was selected because of its centrality in the HR function, its hybrid nature (manual and digital), and its involvement of both internal and external actors.

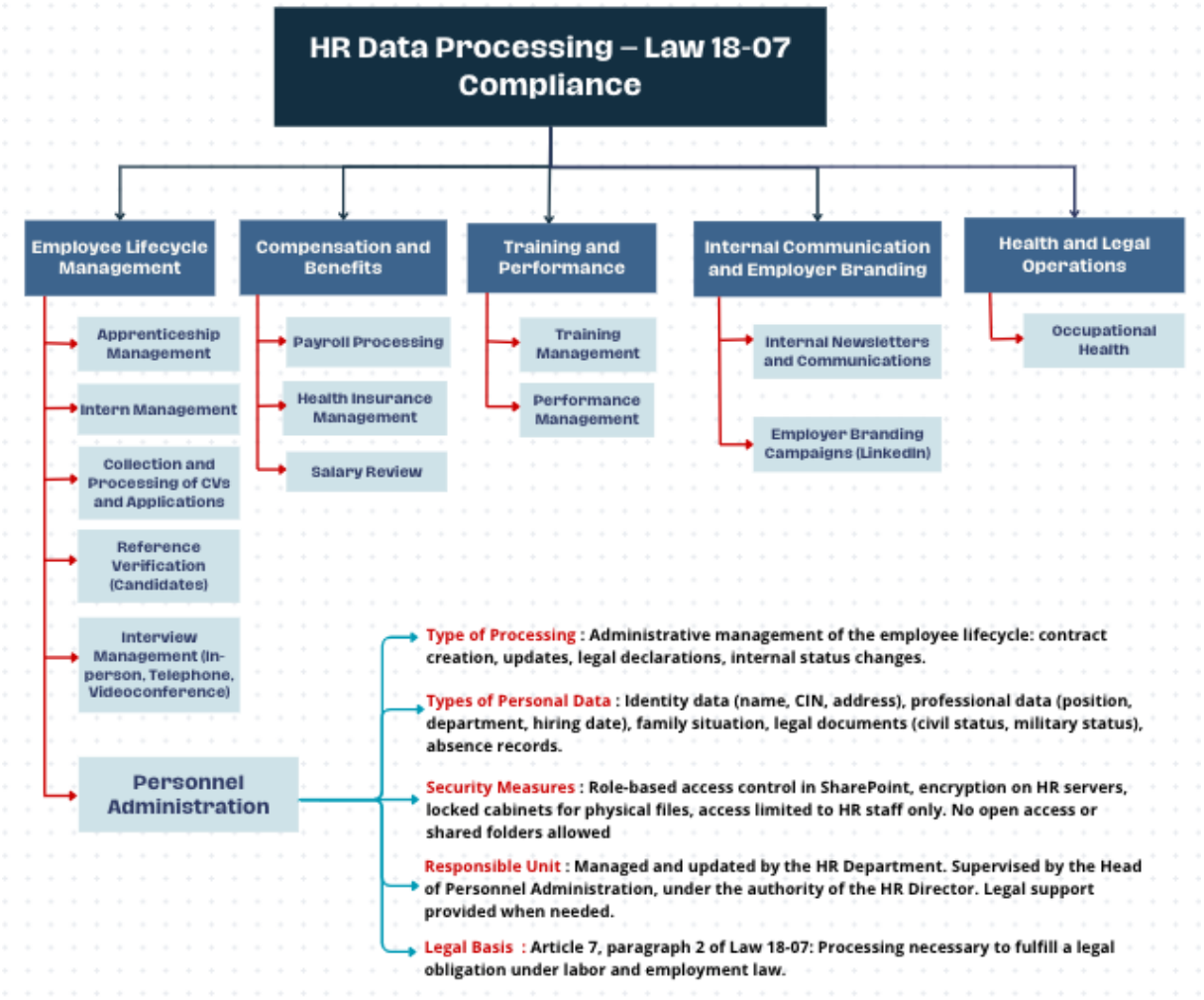
The detailed representation of this processing includes:

- The legal and organizational basis of the operation,
- The categories of personal and sensitive data processed,
- The actors involved (HR, Legal, CNAS),
- The technical and organizational safeguards applied,
- Identified risk areas and improvement recommendations.

The remainder of the HR processing operations are presented at the categorical level without detailed flow, in order to maintain visual clarity.

2.4. mapping of HR Data Processing

Figure 23: Legal and Operational Mapping of Personal Data Processing – HR Department– Personnel Administration



Source : Author's elaboration based on internal documentation, (Cevital, 2024)

This legal cartography allows Cevital to:

- Enhance the internal governance of personal data by clarifying processing lines and responsibilities,
- Facilitate communication with the ANPDP, particularly in the context of declaration or authorization requests,

- Support internal training**,** audits, and risk assessments related to personal data processing,
- Serve as a baseline for the progressive extension of compliance mapping across other departments beyond HR.

The cartography is attached on the following page. It complements the results presented in Section 2.5 and forms the operational and legal foundation for the next phases of Cevital's compliance plan.

Conclusion

The practical part of this thesis demonstrated the importance of aligning internal practices with the legal requirements of Law 18-07. The case study of Cevital highlighted both strengths and areas for improvement in terms of data protection. The mapping and analysis of processing activities in the HR department revealed essential steps for compliance, including documentation, transparency, and internal control mechanisms. This experience confirms that implementing data protection is not only a legal obligation but also a strategic advantage for organizations aiming to build trust and ensure ethical data usage.

General conclusion :

At the conclusion of this research, it becomes clear that the issue of personal data protection now transcends traditional legal and technical boundaries. In Algeria, the acceleration of digital transformation, the proliferation of data processing systems, and increasing regulatory expectations have made compliance a key strategic challenge for public and private institutions alike. In this evolving context, Law No. 18-07, enacted on June 10, 2018, provides a foundational legal framework for governing personal data processing, affirming the primacy of human dignity, transparency, and individual rights.

This thesis was conceived to evaluate the concrete implications of Law 18-07 within an enterprise setting, through a case study focused on Cevital Group, the country's largest private industrial actor. Beyond a legal interpretation of the text, the objective was to explore how the law could be operationalized through internal procedures, cross-functional coordination, and digital tools, in order to meet both regulatory and organizational needs.

To achieve this goal, a dual-method approach was employed:

- On one hand, a legal and documentary analysis of Law 18-07 and the role of the ANPDP, providing the theoretical backbone for understanding regulatory expectations;
- On the other, a field case study at Cevital headquarters, centered on the Human Resources Department, where compliance measures were explored through interviews, simulations, and tool design.

This approach allowed the research to move beyond abstract concepts and into practical implementation, producing a series of outcomes with added value for both the company and the broader Algerian data protection ecosystem.

The work conducted throughout this thesis led to the production of several major outcomes, both theoretical and applied:

- A structured legal mapping of Law 18-07, identifying its seven titles and 74 articles, and offering a thematic breakdown that clarifies obligations, rights, and enforcement mechanisms.

- A detailed study of the role and operational functions of the ANPDP, highlighting its status as an independent authority with a mandate for oversight, guidance, and sanctions.
- The development of a set of internal compliance tools, including:
    - a semi-structured interview guide validated through expert feedback,
    - a bilingual data protection charter,
    - an awareness poster summarizing legal obligations,
    - and a SharePoint-based platform simulating ANPDP declaration forms.
- The successful deployment of the first three phases of the compliance project at Cevital (awareness, inventory, and legal mapping), focused on the Human Resources Department, where 15 data processing operations were identified, analyzed, and documented.
- The creation of a legal and visual data processing cartography, which categorized HR processing activities according to principles such as lawfulness, purpose limitation, actor roles, and retention periods. One operation ("Personnel Administration") was modeled in full.
- The identification of compliance risks, including inconsistent consent management, lack of defined retention periods, and hybrid processing flows (manual/digital) lacking traceability or safeguards.
- The recognition of broader institutional impacts, where the project contributed to building a culture of accountability, transparency, and legal awareness, while strengthening interdepartmental collaboration — a key element of successful digital transformation.

These results validate the thesis's central assumption: compliance with Law 18-07 is not a static legal exercise, but a dynamic and systemic process involving legal knowledge, internal structuring, and strategic foresight.

- **Central Research Problem**

The guiding question of this thesis was:

How can an Algerian enterprise such as Cevital ensure compliance with the legal requirements of Law 18-07 on the protection of personal data?

This problem reflects both the novelty of the legal framework and the complexity of its practical implementation. Rather than treating compliance as a checklist of obligations, the thesis explored it as a strategic, organizational, and multidisciplinary transformation, involving legal clarity, institutional readiness, and operational innovation.

The results of the research demonstrated that effective compliance requires more than an understanding of the legal text. It involves:

- The engagement of leadership and key departments (HR, Legal, IT),
- A rigorous mapping of data processing activities,
- The documentation of legal bases, data flows, actors, and safeguards,
- And a structured interaction with the ANPDP for declarations, guidance, and audits.

Thus, compliance emerges as a continuous and evolving process, requiring not only tools and policies but also internal governance, coordination, and adaptation.

- Q1 – What are the legal and operational requirements of Law 18-07 regarding personal data processing compliance, and how do they justify the need for internal data mapping?

The analysis revealed that Law 18-07 imposes multiple, layered requirements:

- The obligation to have a valid legal basis for each processing operation (Articles 7–10),
- The duty to declare or request authorization for processing from the ANPDP (Articles 29–31),
- The requirement to document operations in an internal register (Article 33),
- And strict standards for transparency, security, and retention, especially in the case of sensitive data (Articles 10, 35, 42).

These elements confirm that data mapping is not optional, but rather a core legal mechanism**.** It is essential for ensuring traceability, facilitating ANPDP declarations, and supporting internal audits.

- Q2 – What internal governance structures were mobilized at Cevital to achieve compliance?

The fieldwork confirmed the establishment of a cross-functional compliance steering model, led by:

- The Human Resources Department, which conducted awareness campaigns and the data processing inventory,
- The Legal Department, which reviewed the regulatory requirements and validated tools,
- The Information Systems Department (DSI), which developed digital tools such as the SharePoint inventory platform.

In addition, departmental focal points were appointed, responsible for identifying, documenting, and reporting processing activities. This internal architecture allowed for both specialization and coordination.

- Q3 – What strategy and project logic did Cevital adopt for compliance?

Cevital adopted a structured seven-phase roadmap, aligned with Law 18-07:

1. Awareness and sensitization,
2. Inventory of data processing operations,
3. Legal qualification and mapping of each operation,
4. Declaration to the ANPDP,
5. Dialogue and feedback from the authority,
6. Integration of recommendations and technical adjustments,
7. Training and institutionalization of procedures.

This approach demonstrates a mature and proactive vision of compliance, treating it not as a constraint, but as a vector of governance improvement and strategic alignment.

- Q4 – What concrete measures and tools were implemented during the project?

Throughout the project, several operational assets were produced:

- A semi-structured interview guide, validated through feedback from the ANPDP,
- A bilingual data protection charter for internal awareness,
- A poster summarizing legal obligations for staff,
- A SharePoint platform to simulate and manage declarations,
- A complete legal mapping methodology, applied to 15 HR processing operations.

These measures laid the groundwork for scalable and repeatable compliance — not only within the HR department, but across the entire organization.

- **Research Results**

The research undertaken in this thesis generated multiple results, both theoretical and empirical. These findings stem from a dual methodology combining legal interpretation and fieldwork and offer insights not only into the formal structure of Law 18-07 but also into its practical implications within a complex organization such as Cevital. This section presents these results thematically, covering the legal foundations, the institutional roles, the operational dimensions of compliance, and the strategic impact of implementing a personal data protection framework.

1. Legal and Institutional Clarification of Law No. 18-07

Before any operationalization could be proposed, it was essential to understand the legal architecture and scope of Law No. 18-07. The analysis undertaken in the first part of the thesis allowed for a comprehensive legal reading of the law and its positioning within the Algerian regulatory ecosystem.

Law 18-07 is built on a coherent legal structure, comprising 74 articles organized across seven thematic titles. These cover the core principles of personal data protection (Articles 1–6), the legal conditions of data processing (Articles 7–16), the creation and role of the National Authority for Personal Data Protection (ANPDP, Articles 17–28), the rights of data subjects (Articles 29–41), and specific rules concerning international data transfers, organizational structure, and sanctions.

Particularly noteworthy are the Articles 7 to 10, which outline the six legal bases for lawful data processing: consent, legal obligation, contractual necessity, protection of vital interests,

public interest, and legitimate interest. These align closely with international standards, particularly the GDPR, while introducing specific obligations regarding declaration and authorization not typically found in European models.

Moreover, the thesis identified the distinct role of the ANPDP as a central institutional actor, endowed with administrative and sanctioning powers. Its missions include registering and authorizing data processing, issuing guidance, conducting audits, and applying penalties in the event of non-compliance. Despite its relatively recent operationalization (in 2022), the ANPDP already holds a foundational place in the national regulatory landscape.

This legal analysis culminated in the creation of a structured legal mapping of Law 18-07, grouped by theme, obligation, and actor responsibility. This mapping served as both a pedagogical framework and a practical reference for the case study conducted within Cevital.

2.Implementation and Field Results at Cevital

The second major axis of the research consisted of an embedded case study conducted within Cevital Group, with a focus on the Human Resources Department. This fieldwork phase enabled the application of the legal framework to actual corporate structures, processes, and challenges.

a) Awareness and Engagement Strategy

One of the first contributions of the fieldwork was the establishment of an internal awareness strategy, designed to sensitize managers and staff to the legal requirements of Law 18-07. A bilingual awareness charter, visual communication tools (such as posters), and a legal summary of obligations were developed and distributed across strategic workspaces. Interviews and meetings were held with key departmental heads, laying the groundwork for project ownership and legal culture within the organization.

This phase also helped to position the project as a cross-functional initiative, moving beyond the legal department to include Human Resources, Information Systems, and operational staff — an essential precondition for sustainable compliance.

b) Inventory and Processing Identification

A core contribution of the thesis was the development of a complete inventory framework to collect and analyze personal data processing activities. This involved the creation of:

- A custom SharePoint platform simulating the declaration process required by the ANPDP,
- Excel templates derived from the 11 official declaration forms of the Authority,
- And a semi-structured interview guide validated by the ANPDP and used with department heads.

Fifteen (15) distinct data processing operations were documented within the HR department, covering sensitive processes such as recruitment, training, medical monitoring, payroll, internal communication, and disciplinary management. Each operation was fully documented in terms of purpose, legal basis, actors, recipients, data sensitivity, retention, and tools used.

c) Legal Analysis and Mapping of Processing Operations

The research produced a comprehensive legal qualification and visual mapping of the documented processing operations. Each entry in the inventory was analyzed using a multidimensional grid:

- Legal basis under Articles 7–10,
- Identification of data subjects and sensitivity of data under Articles 9–10,
- Actors and subcontractors (internal and external),
- Retention periods and justification,
- Means of processing (manual, digital, hybrid),
- Security measures and risk exposure.

A multi-layered cartography was constructed:

1. The first level categorized the HR processes (administrative, medical, contractual),
2. The second identified and described each operation,
3. The third provided a full legal modeling of one representative process: “Administration du personnel”.

This cartography represents a significant academic and operational contribution, translating legal obligations into traceable documentation, ready for ANPDP declaration and internal audits.

d) Identification of Legal and Operational Gaps

The field analysis highlighted several key areas for improvement to strengthen compliance and reduce legal risks, including:

- Establishing comprehensive data retention policies across all processing activities;
- Standardizing consent collection and documentation processes to ensure reliability and compliance;
- Implementing appropriate security and traceability measures for the use of hybrid formats (paper and digital);
- Formalizing and consistently managing data processing agreements with external service providers.

Implementing these enhancements will help reinforce data governance, streamline internal processes, and ensure sustainable compliance with data protection regulations.

- **Strategic, Technical, and Methodological Contributions**

Finally, this research delivered several cross-cutting contributions that go beyond the scope of a legal analysis or an internal audit. These contributions reinforce the strategic and academic value of the thesis:

- **Institutional coordination**: The project served as a bridge between HR, Legal, and IT departments, illustrating the need for multi-disciplinary collaboration in data governance.
- **Tool development and replication**: The interview guide, SharePoint inventory tool, awareness materials, and Excel templates can now be adapted for use in other departments, enabling scalability.
- **Process modeling**: The visual and legal mapping process applied to the HR department created a standardized model for other sensitive departments such as Finance, Audit, or Logistics.

- **Pedagogical value**: The frameworks developed during this thesis can be reused in academic training, legal workshops, or organizational briefings — offering a rare real-world example of Law 18-07 compliance implementation.

In summary, the field research validated the idea that compliance is not merely a legal exercise but a deep organizational transformation. It requires dedicated resources, executive support, clear documentation, digital tools, and above all, a shared understanding of legal responsibilities across all levels of the enterprise.

- **Recommendations**

This thesis has shown that compliance with Law 18-07 is not only a legal imperative but also an organizational opportunity. However, the fieldwork and legal analysis have highlighted several obstacles and limitations. In light of these findings, the following priority recommendations are proposed, grouped by level of responsibility.

- **For the Legal Framework (Law 18-07)**

  - **Clarify the distinction between declaration and authorization**: Many organizations struggle to determine when they need to declare or request formal authorization. A clearer threshold, supported by practical examples, would reduce legal ambiguity.
  - **Introduce Privacy Impact Assessments (PIAs)**: For high-risk processing, PIAs should be required to assess legal, technical, and ethical implications — especially in health, education, or large-scale HR operations.
  - **Facilitate digital procedures**: Declaration and authorization should be done through a user-friendly national platform, allowing for automated tracking, templates, and dashboards.

- **For the ANPDP (National Authority)**

  - **Publish official compliance guides and models**: The ANPDP should issue detailed documentation including model contracts, data inventory templates, and sector-specific instructions (e.g., for HR or healthcare).

- **Develop a certification and training program**: Training internal compliance staff, such as Data Protection Officers (DPOs), would help standardize best practices across Algerian enterprises.
- **Enhance the digital services of the ANPDP**: A responsive online portal with declaration status tracking and messaging functions would make compliance more accessible, especially for large organizations like Cevital.

- **For Companies (Cevital and Others)**

- **Appoint a DPO or dedicated compliance lead**: A central figure responsible for monitoring, updating, and coordinating all personal data processing is essential for sustainable compliance.
- **Replicate the HR pilot across departments**: The mapping, inventory, and tools developed in this research should be scaled to other departments (Finance, Logistics, IT), following the same methodology.
- **Formalize internal procedures and staff training**: A group-wide data protection policy, combined with training for managers and data focal points, would improve awareness and consistency in handling personal data.

By prioritizing these measures, Algerian companies — and public actors — can not only comply with Law 18-07, but also build a data culture based on trust, responsibility, and strategic foresight.

- **Research Hypotheses – Formulation and Assessment**

At the beginning of this research, several working hypotheses were formulated to guide the exploration of the legal, institutional, and operational aspects of Law 18-07. These hypotheses were not meant to be final answers, but rather structured assumptions that could later be tested and refined based on the legal analysis and field investigation conducted within Cevital.

Hypothesis 1 – On Legal Requirements and the Role of Mapping

General conclusion

It was assumed that Law 18-07 primarily emphasizes the principles of personal data protection but does not impose formal internal documentation obligations such as a detailed register or structured processing map.

This hypothesis was refuted. The legal analysis demonstrated that mapping and documentation are not optional — they are explicitly required by Articles 29–35 of the law. The register of processing activities is a central compliance mechanism, and it is through this documentation that controllers must justify their declarations to the ANPDP.

Hypothesis 2 – On Internal Responsibility Structures

It was assumed that compliance with data protection regulations is the exclusive responsibility of the Legal Department and that other departments are only marginally involved.

This hypothesis was also refuted by the field results. The compliance process at Cevital showed that multiple departments — particularly Human Resources and Information Systems — played active and complementary roles. The legal team provided regulatory interpretation, but the HR team led the inventory work, and the DSI developed the SharePoint platform. Compliance was therefore a multidisciplinary effort.

Hypothesis 3 – On the Existence of a Strategic Compliance Approach

It was expected that Cevital approached compliance in an informal or reactive manner, without a long-term strategy or structured roadmap.

This hypothesis was clearly invalidated. The company implemented a seven-phase compliance roadmap, ranging from awareness and inventory to declaration, feedback, and institutionalization. This demonstrates a proactive, project-based approach integrating legal, managerial, and technical dimensions.

Hypothesis 4 – On the Nature of Measures and Tools Developed

General conclusion

It was believed that legal compliance measures at Cevital might be limited to policy documentation and would not involve the development of operational tools or digital platforms.

This assumption was refuted. In practice, the company created multiple operational tools: a SharePoint platform simulating ANPDP forms, Excel templates, a bilingual charter, an awareness poster, and an interview guide. These instruments reflect an advanced level of organizational commitment and offer models for other departments or companies.

In conclusion, while the initial hypotheses reflected common assumptions about regulatory compliance in Algeria, the research has shown that in the case of Cevital, compliance was treated as a structured, multi-actor process — grounded in law, supported by technology, and integrated into the company's broader governance culture.

- **Horizons and Perspectives**

Although this thesis achieved its objectives within the scope of the HR department at Cevital, several extensions remain both at the operational level and within the broader academic and institutional context**.**

- **Internal Continuation at Cevital**

The compliance roadmap designed and partially implemented during the fieldwork still has three important phases to complete:

- **Formal declaration to the ANPDP**, based on the processing inventory and mapping already prepared.
- **Feedback and legal validation**, following ANPDP review.
- **Training and replication**, extending the tools and methods developed (interview guide, SharePoint platform, templates) to other departments.

These steps are essential to complete the cycle of compliance and ensure long-term integration of Law 18-07 within the company.

- **Broader Organizational and Strategic Extensions**

The methodology developed can be **replicated** in other Algerian organizations. The project thus becomes:

- A **pilot model** for other departments at Cevital (Finance, IT, Logistics),
- A **benchmark** for national enterprises seeking to operationalize Law 18-07,
- A **basis for harmonizing third-party contracts** with subcontractors and service providers.

- **Academic and Legal Research Perspectives**

From a research standpoint, this thesis opens promising directions:

- **Comparative studies** between Law 18-07 and international regulations (e.g., GDPR),
- **Studies on employee behavior and awareness** regarding data protection,
- **Development of digital compliance tools**, such as inventory dashboards or risk alerts.

These future works could help shape an emerging academic field in Algeria around data governance and digital law.

Bibliography

- **Books**

- Voigt, P. &. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Vol. 1). (S. I. Publishing, Éd.) Cham, Canton de Vaud , Suisse: Springer International Publishing.
- Carey, P. (2018). *Data Protection: A Practical Guide to UK and EU Law* (Vol. 1). (B. Professional, Éd.) London, United Kingdom: loomsbury Professional.
- Ustaran, E. (2018). *European Data Protection: Law and Practice* (Vol. 1). (IAPP, Éd.) London, United Kingdom : IAPP (International Association of Privacy Professionals).

- **Scientific Articles**

- Greenleaf, G. (2011, Septembre). Global Data Privacy Laws: Forty Years of Acceleration. *Privacy Laws & Business International Report*(112), pp. 11–17.
- Binns, R. (2018). Data Protection by Design and by Default: The GDPR's Approach to Profiling and Automated Decisions. *Computer Law & Security Review, 34*(6), pp. 1234-1253.
- Gunuganti, R. (2018). Privacy and data protection in the digital age. *Journal of Social and Economic Research, 5*(12), pp. 358–365.
- Redman, T. C. (1998, Février). The impact of poor data quality on the typical enterprise. *Communications of the ACM, 41*(2), pp. 79–82.

- **Reports**

- Cavoukian, A. (2013). *Privacy by Design: The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario. Toronto: Information and Privacy Commissioner of Ontario.

- Autorité nationale de protection des données à caractère personnel [ANPDP]. (2025). *Guidelines on security measures.* Consulté le juin 2025, sur ANPDP: https://anpdp.dz
- CNIL & Délégation Algérienne. (2021). *Étude comparative entre la loi 18-07 et le RGPD européen.* Commission Nationale de l'Informatique et des Libertés (CNIL). Paris: CNIL.

- **Regulatory Texts**

- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* European Parliament and Council of the European Union, Official Journal of the European Union. Brussels: Official Journal of the European Union.
- République Algérienne Démocratique et Populaire. (2018). *Loi n° 18-07 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.* Gouvernement Algérien, Ministère de la Justice. Alger: Journal Officiel de la République Algérienne .
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2019). *ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* ISO / IEC. Genève: ISO.

- **Websites**

- Karjian, M. (2024, avril). *What is Data Protection and Why is it Important?* Consulté le juin 2025, sur TechTarget: https://www.techtarget.com/whatis/definition/data-protection
- Marketing Intervalle. (2024, avril 25). *Loi 18-07 : les défis de la protection des données personnelles.* Consulté le juin 2025, sur Intervalle Technologies: https://intervalle-technologies.com/blog/loi-18-07-protection-donnees-personnelles
- European Commission. (s.d.). *What is data processing?* Consulté le 06 2025, sur European Commission: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

- Cevital. (s.d.). *Accueil.* Consulté le juin 2025, sur Cevital: https://www.cevital.com/

- **Miscellaneous**

- BACHIR, T. (2024, décembre 11). *Le "Point Focal" ou DPO : un acteur clé de la protection des données en Algérie.* Récupéré sur LinkedIn: https://www.linkedin.com/pulse/le-point-focal-ou-dpo-un-acteur-cl%C3%A9-de-la-protection-des-bachir-scbkf/
- Cevital. (2024, avril 15). Plan stratégique de gouvernance des données. Alger , Alger , Algérie: Cevital.

Appendix

- **Appendix A – Legal Interview Guide and Summary Report**

Dans le cadre du mémoire de fin d'études sous le thème :

Analyse et cartographie des traitements des données à caractère personnelles dans le cadre de laconformité à la loi 18-07

RÉALISÉ PAR : BENAIDA Meriem

Master 2 spécialité Management Digital

mbenaida_etd@esgen.edu.dz

École Supérieure De Gestion Et D'économie Numérique

Le : 26/11/2024

Introduction

- **Objectif de l'entretien**

  L'objectif de cet entretien est d'obtenir des informations vérifiables sur les pratiques de l'ANPDP en matière de conformité à la loi 18-07, dans le cadre du mémoire de fin d'études susmentionné. Il vise à analyser les mécanismes de gestion et de protection des données personnelles en Algérie, tout en identifiant les initiatives liées à la mise en œuvre de cette loi.

- **Contexte**

  L'ANPDP a été instituée par la loi 18-07 pour assurer la régulation et la protection des données personnelles en Algérie. Son rôle principal est de garantir le respect des droits des individus en matière de données personnelles, conformément aux régles établies par cette loi. Cet entretien a pour but d'examiner les missions de l'ANPDP, les défis rencontrés dans leur mise en œuvre, ainsi que les actions entreprises pour accompagner les entreprises dans leur conformité légale.

- **Méthodologie**

  Cet entretien adopte une approche semi-structurée, avec des questions ouvertes permettant de recueillir des réponses précises tout en laissant la liberté à l'interviewé de s'attarder sur les points qu'il juge pertinents. Les questions ont été conçues pour explorer la mise en œuvre de la loi 18-07 et le rôle de l'ANPDP dans ce processus.

Liste des réponses

I. Présentation de l'ANPDP

1) Définition et Mission :**Pouvez-vous décrire brièvement l'ANPDP, ses missions principales, et sa structuration interne pour accomplir ses objectifs ?**

L'Autorité Nationale de Protection des Données Personnelles (ANPDP) est une autorité administrative indépendante chargée de veiller à la protection des données personnelles. Créée pour veuiller sur l'application de la loi 18-07, son but est de préserver les droits et libertés des individus en matière de vie privée et de données personnelles qui sont traitées par les personnes physiques et les secteurs public et privé.

Désignation & installation des membres de l'ANPDP, dont le Président

L'ANPDP est composée de 16 membres dont le président, spécialisés dans le domaine technique et juridique :

- **Ils sont nommés pour une durée de cinq (5) ans en vertu du décret présidentiel 22-187 du 18 mai 2022.**
- **Ils ont été installés jeudi 11 août 2022 à la Cour suprême.**
- **Ils ont prêté serment le mardi 30 août 2022 à la Cour d'Alger.**

Elle est dotée d'un secrétariat exécutif composé de plusieurs directions spécialisées dans les domaines technique, juridique et administrative pour gérer divers aspects de la protection des données.

Interlocuteurs :

- Mr. Hacene Boualem, membre de l'Autorité Nationale de Protection des Données Personnelles et Directeur des études.
- 5 cadres spécialisés dans le domaine juridiques et informatiques.

2) Rôles et ResponsabilitÉs : **Quels sont les rôles principaux de l'ANPDP pour garantir le respect de la loi 18-07 sur la protection des données personnelles en Algérie ?**

Les principales fonctions de l'ANPDP sont axées sur la surveillance, l'encadrement, et l'application de la conformité avec la loi 18-07. Voici un aperçu de ses missions citées dans l'article 25 de la loi :

- délivrer les autorisations et de recevoir les déclarations, les réclamations, les recours et les plaintes,
- informer les personnes concernées et les responsables de traitement de leurs droits et obligations,
- réaliser les opérations d'audit et de contrôle au niveau des locaux du responsables de traitement,

- ❖ développer et promouvoir la coopération nationale et internationale dans son domaine d'activité.

3) DÉFIS RONCONTRÉS : **Quelles sont les principales difficultés rencontrées par l'ANPDP dans l'application de la loi 18-07 depuis son entrée en vigueur ?**

Depuis sa création en août 2023, l'ANPDP (Autorité Nationale de Protection des Données Personnelles) a entrepris plusieurs initiatives pour mettre en œuvre la loi 18-07 relative à la protection des données personnelles. Voici les principaux défis auxquels elle fait face dans l'application de cette loi :

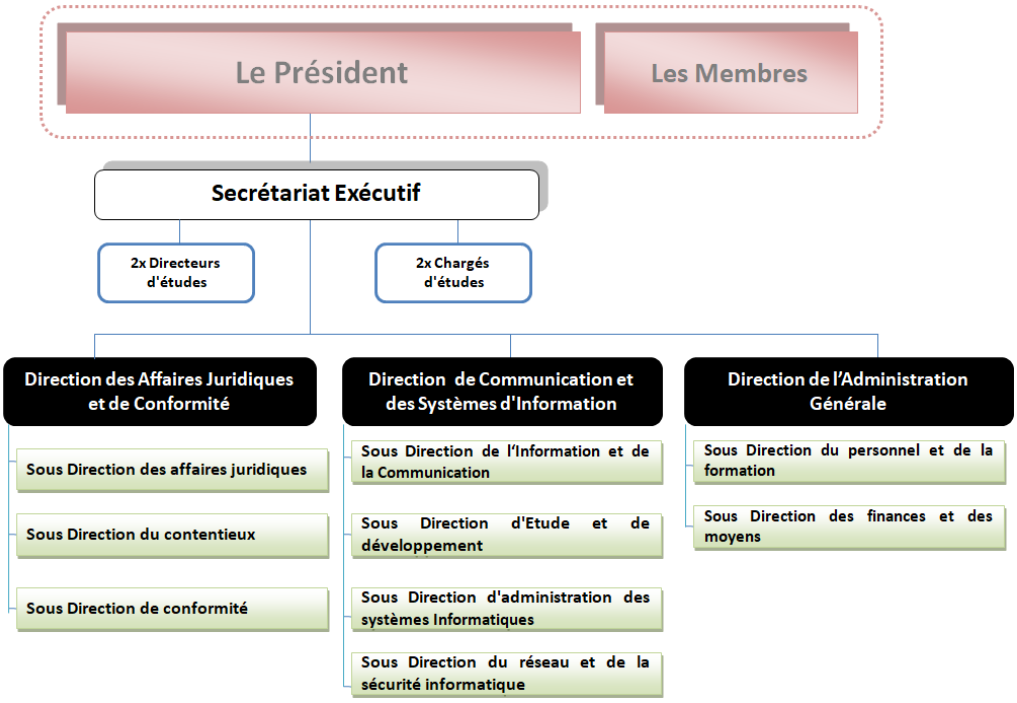
1. L'ampleur et la diversité des missions : L'ANPDP doit accomplir de nombreuses missions de régulation, de sensibilisation, et de contrôle dans un contexte où la culture de la protection des données personnelles reste peu développée dans de nombreux secteurs en Algérie.

2. Mise en place des textes réglementaires : À la suite de l'installation de ses membres, l'ANPDP a élaboré des textes réglementaires pour encadrer l'application de la loi 18-07. Ces textes sont essentiels pour fournir un cadre clair aux institutions et entreprises et ont exigé du temps et des ressources importantes.

3. Lancement des outils numériques : Afin de faciliter la gestion des données et d'accompagner les organismes vers la conformité, l'ANPDP a développé son site web (www.anpdp.dz) un portail numérique (https://portail.anpdp.dz/) destinés aux organismes public et privé concernés par conformité avec la loi 18-07. Son site web est très riche en informations notamment pour les modalités de conformité avec la loi et des gides de formation sur la loi 18-07 ainsi qu'un espace de communication des activités de l'ANPDP.

Aussi, l'ANPDP dispose d'une page facebook (https://www.facebook.com/anpdp.dz?locale=fr_FR)

4. Organisation de l'ANPDP



5. Réception et traitement des dossiers : Depuis septembre 2024, l'ANPDP a commencé à recevoir des dossiers, incluant les déclarations de traitement de données, les demandes d'autorisation et les demandes d'avis. Gérer ces demandes et s'assurer que toutes répondent aux exigences légales constitue un défi organisationnel majeur.

6. Sensibilisation des secteurs : Pour pallier le manque de culture de protection des données, l'ANPDP a initié des campagnes de sensibilisation, notamment sous forme de tables rondes avec les représentants des différents secteurs ministériels. De janvier à mai 2024, ces réunions ont permis d'informer et de sensibiliser les parties prenantes aux enjeux de la loi 18-07.

7. Communication adaptée et spécialisée : L'ANPDP a mis en place deux adresses électroniques spécifiques pour répondre aux besoins des organismes :

- Adresse juridique : '' juridique@anpdp.dz '' pour toutes les questions réglementaires.
- Adresse technique : ''technique@anpdp.dz '' pour le support technique et les questions de sécurité.

Ces canaux permettent une communication efficace et ciblée avec les parties prenantes, en fonction de leurs besoins spécifiques.

8. Organisation de séminaires et de conférences : L'ANPDP organise des séminaires et des conférences, soit directement, soit en intervenant dans ceux organisés par des secteurs comme le secteur bancaire. Ces événements permettent de diffuser des informations précises sur la loi et d'encourager la mise en conformité.

9. Formation des responsables et employés des organismes : Pour accompagner les entreprises dans leur mise en conformité, l'ANPDP a conçu un programme de formation couvrant les aspects essentiels de la loi, incluant :

- Un résumé des dispositions clés de la loi 18-07 ;
- Les obligations des responsables de traitement de données ;
- Les solutions techniques disponibles pour la déclaration et la mise en œuvre de la conformité, avec un appui au niveau du secrétariat exécutif.

10. Demande croissante de rendez-vous : Le besoin d'assistance en matière de protection des données est en pleine expansion, et l'ANPDP reçoit de nombreuses demandes de rendez-vous. Cette forte demande souligne l'intérêt des entreprises pour la conformité mais représente également une pression sur les ressources humaines et logistiques de l'ANPDP.

11. De plus, il convient de noter que l'ANPDP s'appuie sur le cadre juridique prévu par la Constitution algérienne, notamment l'article 41, alinéa 4 du **Dahir 2020**, qui consacre le droit de chaque individu à la protection de ses données personnelles. Ce texte fonde l'obligation de l'État et des institutions à garantir la protection de la vie privée, et renforce l'application de la loi 18-07. En ce sens, l'ANPDP joue un rôle clé dans la mise en œuvre des principes énoncés dans cette disposition constitutionnelle.

II. Conformité Légale et Pratiques

4) Exigences pour le Transfert de Données : **Quelles sont les conditions imposées par l'ANPDP pour le transfert de données personnelles à l'étranger, notamment en ce qui concerne l'hébergement sur le cloud ?**

En conformité avec la loi 18-07 relative à la protection des données personnelles et ses articles 38 et 39, ainsi que le **Guide National de Sécurité Informatique (RNC 2020)**, les conditions de transfert à l'étranger se distinguent selon plusieurs cas spécifiques.

- Conditions générales pour tout transfert de données

1. Conformité réglementaire

- Le pays destinataire doit disposer d'une réglementation équivalente ou compatible avec les lois algériennes, notamment en matière de protection des données personnelles.
- Une autorité nationale dédiée à la protection des données doit exister dans ce pays.

2. Documentation légale obligatoire

- La société ou entité destinataire doit fournir un contrat ou une certification garantissant le respect des normes algériennes.

3. Interdiction stricte pour les organismes publics

- Aucune donnée ne peut être transférée à l'étranger par les institutions publiques, conformément au **RNC 2020**, sauf cas exceptionnel approuvé par le Conseil National.

4. Autorisation préalable de l'ANPDP

- Chaque demande de transfert doit obtenir une validation explicite de l'ANPDP, fondée sur une analyse approfondie des risques.

- Cas spécifiques pour le transfert de données

1. Transferts entre filiales et maison-mère étrangère

- Lorsqu'une entreprise en Algérie est liée à une maison-mère étrangère :
- Le ‘’ contrat de base ’’ doit être enregistré et validé par un notaire.
- Les règles de transfert incluent une vérification du ‘’ statut juridique’’ des parties impliquées.
- Si une maison-mère détient une majorité de parts et gère les opérations de ses filiales, elle peut demander des données, à condition de fournir une documentation conforme.

2. Utilisation de services cloud (sous-traitance)

- Lorsqu'un traitement de données est effectué via des solutions cloud :
- Un ‘’ contrat de sous-traitance ’’ est obligatoire, définissant clairement les responsabilités des parties.
- Le ‘’ Guide de Formation n°2 ’’ , mentionné dans le cadre réglementaire, précise les exigences techniques et contractuelles liées aux sous-traitants.
- Des mesures de sécurité comme le chiffrement des données et des audits réguliers doivent être mises en place.

3. Partage entre branches d’un même groupe multinational (bancaire ou autre)

-(Par exemple, une banque multinationale transférant des données entre ses branches) :

- Les ‘’ Conditions Générales de Gestion (CCG) ‘’ doivent inclure des protocoles spécifiques pour le transfert, garantissant la protection des données.

- Le système ‘’ SESA ‘’ (Système d’Échange Sécurisé Algérien) est requis pour assurer un transfert conforme aux standards locaux.

- Un ‘’ addendum ‘’ pour la protection des données personnelles doit être intégré au contrat principal, basé sur les normes de la maison-mère.

- Critères supplémentaires obligatoires

1. Assurance de sécurité

- Le sous-traitant ou destinataire des données doit démontrer sa capacité à appliquer des mesures techniques et organisationnelles conformes (chiffrement, protocoles d'accès restreint).

2. Garanties spécifiques pour les données sensibles

- Les données financières, médicales ou sensibles nécessitent des protocoles supplémentaires, incluant des vérifications régulières de conformité.

3. Compatibilité légale et technique

- Le transfert n’est permis que si le pays destinataire dispose d'une législation et d’une infrastructure technique compatible avec le cadre algérien.

Ces exigences montrent que l’ANPDP adopte une approche rigoureuse pour réguler les transferts internationaux de données, garantissant la souveraineté numérique et la sécurité des citoyens algériens

5) Démarches de Conformité : **Quelles étapes clés une entreprise doit-elle suivre pour déclarer et obtenir une licence pour le traitement des données personnelles ?**

Étapes clés pour déclarer et obtenir une licence pour le traitement des données personnelles

1. Préparation de la cartographie des traitements des données personnelles

La première étape consiste à préparer une cartographie complète des traitements des données personnelles réalisés au sein de l'entreprise. Cela doit être formalisé sous forme de document et comprend toutes les informations sur les processus de collecte, d’utilisation, de stockage et de partage des données. Cette cartographie est essentielle pour identifier les risques associés aux traitements et pour s’assurer de leur conformité avec la loi.

2. Demande de consentement initial

Une fois la cartographie préparée, l’entreprise doit obtenir un consentement préalable de l'ANPDP. Cela implique la soumission d’une demande formelle de traitement des données, avec toutes les informations nécessaires sur les finalités et les mesures de sécurité mises en place.

3. Rédaction du procès-verbal de demande

Après la demande de consentement, un procès-verbal est rédigé, qui est un document officiel précisant les actions et décisions prises en matière de protection des données. Ce procès-verbal est essentiel pour formaliser l'accord et garantir la transparence du processus.

4. Décision de l'ANPDP

L'ANPDP examine la demande et prend une décision : elle peut autoriser ou non le traitement des données personnelles. Cette décision est basée sur la conformité du traitement avec la législation en vigueur, les garanties de sécurité mises en place, et le respect des droits des personnes concernées.

5. Déclaration dans l'espace de travail interne

Une fois l'autorisation accordée, l'entreprise doit procéder à la déclaration du traitement des données personnelles à l'intérieur de l'espace de travail, afin d'en informer toutes les parties prenantes. Cette étape assure que l'ensemble des employés et des responsables comprennent les modalités de traitement des données et les obligations associées.

6) Ressources disponibles pour la conformité : **Existe-t-il une '' checkliste de conformité '' ou un document officiel élaboré par l'ANPDP pour valider les traitements des données a caracters personnelles ?**

Les entreprises doivent respecter plusieurs obligations légales pour garantir la conformité avec la loi 18-07 relative à la protection des données à caractère personnel. Ces obligations sont listées sur la page officielle de l'ANPDP intitulée "Quelles sont vos obligations", disponible via ce lien : (https://anpdp.dz/fr/quelles-sont-vos-obligations/) .

De plus, l'ANPDP a élaboré un document spécifique, le Guide de Formation n°4, intitulé "Comment se conformer à la loi 18-07". Ce guide est un outil clé pour accompagner les organisations dans leur mise en conformité. Il détaille :

- Les étapes à suivre pour structurer un traitement conforme ;
- Les exigences à respecter pour la collecte, le stockage et la gestion des données ;
- Les bonnes pratiques à adopter pour garantir la sécurité et la confidentialité des données.

Ce guide est téléchargeable directement depuis le site de l'ANPDP à ce lien : (https://anpdp.dz/wp-content/uploads/2024/07/Guide-de-formation-N%C2%B04-comment-se-conformer-a-la-loi-18-07-ANPDP.pdf) .
Ces ressources permettent aux responsables de traitement de comprendre les exigences légales et de s'assurer que leurs pratiques respectent les dispositions de la loi 18-07.

III. Communication et Soutien aux Entreprises

8) Mécanismes de Communication : **Quels canaux l'ANPDP utilise-t-elle pour interagir avec les entreprises privées, et quelle est la fréquence de ces échanges ?**

Mécanismes de Communication de l'ANPDP avec les Entreprises Privées

1. Canaux de communication disponibles

L'Autorité Nationale de Protection des Données Personnelles (ANPDP) met à disposition plusieurs moyens pour interagir avec les entreprises privées :

- Adresses e-mail officielles :

Trois e-mails sont spécifiquement dédiés à la communication avec les entreprises et peuvent être trouvés sur le site officiel de l'ANPDP :

- '' contact@anpdp.dz '' (pour les demandes générales).
- '' autorisation@anpdp.dz '' (pour les demandes d'autorisation liées aux transferts ou traitements de données).
- '' support@anpdp.dz '' (pour toute assistance technique ou problème lié aux données personnelles).

- Demandes de rendez-vous ou d'entretien

Les entreprises peuvent également soumettre des demandes de rendez-vous physiques ou virtuels avec des responsables de l'ANPDP pour discuter de sujets spécifiques. Ces demandes peuvent être faites via les e-mails mentionnés ou directement sur le site officiel.

2. Fréquence des échanges : Pas de fréquence limitée

Les échanges entre l'ANPDP et les entreprises privées ne sont pas soumis à une fréquence prédéfinie. Ils dépendent des besoins des entreprises, notamment pour :

- La soumission de nouvelles demandes d'autorisation.
- Les signalements d'incidents ou violations de données.
- Les suivis de conformité aux réglementations en vigueur.

3. Outils complémentaires de communication

- Portail officiel

Le site de l'ANPDP offre un accès direct à des ressources, des formulaires, et des guides pratiques pour faciliter les interactions.

- Présence physique et téléphonique

Les entreprises peuvent également interagir via des visites aux bureaux de l'ANPDP ou en contactant leur numéro de téléphone '' +213 (23) 477 300 ''pour des demandes urgentes.

9) Formation et Sensibilisation : **Quels types de formations et de campagnes de sensibilisation l'ANPDP propose-t-elle pour aider les entreprises à se conformer à la loi 18-07 ?**

Pour garantir la conformité à la loi 18-07, qui régit la protection des données personnelles en Algérie, l'Autorité Nationale de Protection des Données Personnelles (ANPDP) a mis en place

une série de programmes de formation et de sensibilisation pour les entreprises. Voici les principaux moyens mis à disposition pour accompagner les entreprises

1. Espace de formation dédié

L'ANPDP dispose d'un espace de formation spécifique où les entreprises peuvent envoyer leurs responsables et collaborateurs pour des formations approfondies. Cet espace permet d'aborder en détail les bonnes pratiques et les obligations légales en matière de protection des données.

2. Rencontres sur demande

Les entreprises peuvent solliciter des rencontres personnalisées auprès de l'ANPDP. Ces réunions permettent de répondre aux besoins spécifiques des entreprises, avec un accompagnement personnalisé sur des aspects précis de la conformité. Ces rencontres se font en fonction des disponibilités, et les entreprises peuvent prendre contact par les canaux fournis pour organiser ces sessions.

3. Assistance aux questions fréquentes

L'ANPDP est disponible pour répondre aux questions des entreprises concernant leurs responsabilités et droits liés à la protection des données. Elle offre un service de réponse aux questions fréquemment posées, que les entreprises peuvent consulter en ligne ou obtenir par email pour faciliter leur compréhension des aspects techniques et juridiques.

4. Sessions de formation formelles

En plus de l'espace de formation et des rencontres spécifiques, des sessions formelles de formation sont organisées régulièrement. Ces formations abordent divers thèmes relatifs à la loi 18-07, y compris la sécurité des données, les processus de gestion des données, et les mesures de conformité.

5. Site web et page Facebook de l'ANPDP

L'ANPDP diffuse des informations essentielles et des mises à jour régulières via :

- Le site officiel : [anpdp.dz](https://www.anpdp.dz) — une plateforme où sont publiés des guides, des documents réglementaires, des actualités, et des conseils pratiques pour se conformer aux normes de protection des données.
- La page Facebook :

[Page Facebook del'ANPDP] (https://www.facebook.com/anpdp.dz) — cette page sert de canal de sensibilisation où l'ANPDP partage des vidéos éducatives, des informations sur les formations à venir, et des articles de sensibilisation. La page est régulièrement mise à jour pour toucher un large public et maintenir les entreprises informées des dernières évolutions.

6. Reportages et interventions télévisées

L’ANPDP participe activement à des émissions télévisées et des reportages afin de sensibiliser le public aux enjeux de la protection des données. Ces interventions permettent de toucher un large public, d’expliquer les dispositions de la loi 18-07, et d’encourager les entreprises à adopter les bonnes pratiques.

Coordonnées de l'ANPDP pour les entreprises

Les entreprises peuvent contacter l’ANPDP via les adresses email disponibles sur le [site officiel] (https://www.anpdp.dz), ainsi que par téléphone pour obtenir des informations spécifiques ou planifier des sessions de formation et de sensibilisation. Voici les informations principales :

- Emails de contact : Trois adresses sont mises à disposition pour des échanges spécifiques (détaillées sur le site officiel).
- Numéro de téléphone : Le numéro de téléphone est disponible dans la section de contact du site [anpdp.dz](https://www.anpdp.dz).

10) Exemples Concrets : **Pourriez-vous partager des exemples de cas où l'ANPDP a aidé des entreprises à se conformer, ou des cas où des entreprises ont rencontré des difficultés ?**

En raison des règles de confidentialité et de la nature sensible des informations traitées, l'ANPDP ne peut pas divulguer de détails spécifiques sur les cas d'accompagnement ou de difficultés rencontrées par les entreprises. Toutefois, l'ANPDP s'efforce toujours d'apporter son soutien aux entreprises dans le cadre de leur mise en conformité en fournissant des orientations générales et des recommandations sur les bonnes pratiques

IV. Rôle et Responsabilités

11) Rôle du DPO : **Pouvez-vous détailler le rôle et les responsabilités du Délégué à la protection des données (DPO) et ses relations avec l'ANPDP ?**

Le Délégué à la Protection des Données (DPO) occupe un rôle central pour assurer la conformité de l’entreprise à la ‘’ loi 18-07 ’’ sur la protection des données personnelles, comme stipulé dans les ‘’ articles 73 à 78 ‘’ et renforcé par les décrets d’août 2024

1. Garantie de la Conformité et Veille Réglementaire

- Le DPO doit s'assurer que les pratiques de l'entreprise sont conformes aux articles 73-78 de la loi, en intégrant les principes de confidentialité dès la conception des projets et en effectuant des contrôles réguliers pour maintenir cette conformité.

- Il assure également une ‘’ veille réglementaire ‘’ pour anticiper et adapter les politiques internes aux évolutions légales en matière de protection des données.

2. Processus de Nomination et Déclaration d’Honneur

- Pour formaliser sa prise de fonction, le DPO doit signer une ‘’ déclaration d’honneur ‘’, laquelle est soumise à l'ANPDP. Cette déclaration confirme son engagement à agir de manière responsable et transparente.
- L'ANPDP approuve ensuite la nomination, notifiant officiellement l’entreprise que le DPO est habilité à remplir ce rôle.

3. Gestion des Violations de Données

- En cas de ‘’ violation de données ‘’ (intrusion, perte de données, etc.), le DPO est chargé de notifier l'ANPDP dans les plus brefs délais.
- Il doit transmettre un ‘’ rapport complet ‘’ détaillant les informations affectées, la date de l'incident, les actions correctives appliquées, et les conséquences potentielles. Ces informations sont consignées dans un ‘’ registre des incidents ‘’, essentiel pour démontrer la réactivité de l’entreprise face aux risques de sécurité.

4. Réalisation d’Audits et Contrôles Périodiques

- Le DPO mène des ‘’ audits réguliers ‘’ pour s'assurer que les pratiques de l’entreprise restent conformes aux exigences de l’ANPDP. Ces audits peuvent être planifiés ou inopinés et visent à évaluer la sécurité des systèmes et des données personnelles traitées.

5. Sensibilisation et Formation du Personnel

- Le DPO joue un rôle clé dans la ‘’ sensibilisation du personnel ‘’ aux bonnes pratiques de gestion des données, à travers des sessions de formation et des rappels sur la confidentialité et la sécurité.
- Il répond également aux questions internes pour guider le personnel dans la compréhension et l'application des normes de protection des données.

6. Relations avec l’ANPDP

- En tant qu’intermédiaire officiel entre l’entreprise et l’ANPDP, le DPO facilite les échanges et garantit que l’entreprise reste à jour sur les recommandations de l'ANPDP. Cela inclut la gestion des communications et des demandes de mise en conformité.

12) Manuel d'Audit : **L'ANPDP propose-t-elle un manuel ou un cadre type pour aider les entreprises à auditer leur conformité et diagnostiquer leurs processus ?**

L’Autorité Nationale de Protection des Données Personnelles (ANPDP) n’a pas encore publié de manuel d’audit spécifique pour les entreprises. Cependant, les entreprises algériennes peuvent

s’inspirer des pratiques de conformité appliquées dans le cadre du RGPD européen, ainsi que d’autres méthodes d’audit

1. Règlement Général sur la Protection des Données (RGPD) :

Le RGPD européen fournit un cadre exhaustif pour la protection des données personnelles et peut être une référence importante pour les entreprises algériennes en raison de la similarité entre la loi 18-07 et le RGPD. Ce règlement établit les bases de la collecte et du traitement des données, les droits des personnes concernées, et les responsabilités des organisations. Les entreprises peuvent y trouver des lignes directrices sur la sécurité, la transparence, et la gestion des données sensibles. Par exemple, des concepts comme la minimisation des données, la transparence dans l'utilisation des données, et les droits des utilisateurs (accès, modification, suppression) sont fondamentaux dans les deux législations.

2. Étude de l’Impact sur la Vie Privée (Privacy Impact Assessment, PIA) :

Le PIA, ou analyse d'impact relative à la protection des données, est une évaluation qui aide les entreprises à identifier les risques associés aux traitements de données susceptibles d’impacter la vie privée. Ce type d'évaluation est particulièrement pertinent lors de l'implémentation de nouvelles technologies ou d'opérations de traitement de données importantes. Il comprend des étapes comme l'identification des risques potentiels, l’évaluation des conséquences sur la vie privée, et la mise en place de mesures pour atténuer ces risques. Les entreprises peuvent élaborer un PIA pour chaque nouveau processus de collecte de données afin de mieux gérer et prévenir les risques.

3. Protocole et Méthodologie d’Audit :

En l'absence de manuel propre à l'ANPDP, les entreprises peuvent s'appuyer sur des protocoles d’audit déjà disponibles et appliqués au niveau international. Un audit de protection des données peut inclure la vérification des processus internes de collecte, stockage et traitement des données, ainsi que le respect des droits des individus. Un protocole type d’audit inclut généralement :

- Préparation : Étude des lois et des standards de conformité pertinents.
- Audit sur le terrain : Vérification des pratiques de traitement de données, des systèmes de sécurité et de l’accès aux données.
- Évaluation des non-conformités : Identification des écarts par rapport aux standards et des risques associés.
- Recommandations et actions correctives : Proposition de mesures pour renforcer la conformité et prévenir les violations.

4. Bonnes Pratiques en matière de Protection de la Vie Privée:

L’ANPDP recommande des pratiques qui minimisent les risques pour la vie privée lors de la gestion des données personnelles. Ces bonnes pratiques incluent :

- Minimisation des Données : Recueillir uniquement les données nécessaires et les conserver pour une durée limitée.

- Transparence : Informer les individus des finalités du traitement de leurs données et obtenir leur consentement lorsque c'est requis.

- Sécurité des Données : Mettre en place des mesures de sécurité adéquates (ex. : chiffrement, contrôle des accès) pour protéger les données contre les accès non autorisés ou les violations.

- Registre des Traitements : Documenter tous les traitements de données dans un registre, un outil indispensable pour suivre et auditer les pratiques de l'entreprise.

13) Processus de nomination des responsables de traitement : **Concernant le processus de nomination des responsables des traitements, est-il possible de disposer d'un modèle officiel de Déclaration d'Honneur , sachant qu'il n'est pas publié sur le site web de 'ANPDP ?**

Lors de la nomination d'un responsable de traitement, l'ANPDP exige une Déclaration d'Honneur, qui fait partie intégrante du processus d'enregistrement. Cette déclaration est incluse dans un formulaire électronique disponible sur le portail officiel de l'ANPDP (https://portail.anpdp.dz/index.php?page=inscription)

Le formulaire doit être rempli lors de la création d'un compte sur le portail, et il contient :

- Une déclaration formelle de conformité à la loi 18-07 ;
- L'engagement du responsable de traitement à respecter les principes de protection des données personnelles ;
- Une confirmation de la véracité des informations fournies lors de l'enregistrement.

Ce processus numérique simplifie l'accès au portail et garantit que les responsables de traitement adhèrent aux obligations légales dès le début de leur activité. En l'absence d'un modèle téléchargeable, ce formulaire constitue la base officielle pour formaliser la nomination et s'assurer de la conformité des responsables.

IV. Innovations et Perspectives

14) Adaptation aux Technologies Émergentes : **Comment l'ANPDP anticipe-t-elle l'impact des technologies émergentes sur la protection des données personnelles ?**

L'ANPDP (Autorité Nationale de Protection des Données à Caractère Personnel) s'engage activement à anticiper l'impact des technologies émergentes, telles que l'intelligence artificielle, l'Internet des objets (IoT) et les technologies de cloud computing, sur la protection des données personnelles. L'autorité suit plusieurs stratégies clés pour garantir que ces innovations respectent la confidentialité des données et les droits des individus

1. Surveillance et évaluation des risques : L'ANPDP surveille activement les nouvelles technologies et évalue leurs implications pour la protection des données personnelles. Cela inclut la gestion des risques associés à l'automatisation des processus, aux systèmes de traitement de données massives et aux nouvelles pratiques de collecte de données, telles que celles liées aux dispositifs IoT.

2. Adaptation du cadre législatif : L'ANPDP œuvre à la mise à jour des réglementations et des lignes directrices pour intégrer les défis posés par les technologies émergentes tout en respectant la loi 18-07 relative à la protection des données personnelles. Ces réglementations s'inspirent des standards internationaux, notamment le RGPD, tout en tenant compte des spécificités locales.

3. Formation et sensibilisation des entreprises: L'ANPDP met en place des sessions de formation, des séminaires et des campagnes de sensibilisation pour aider les entreprises à comprendre les implications légales des technologies émergentes et à mettre en œuvre des pratiques de gestion des données conformes. Ces efforts visent à réduire les risques de violations des données et à promouvoir des pratiques responsables de collecte et de traitement des données.

4. Collaboration internationale : L'ANPDP participe activement aux discussions internationales sur la protection des données personnelles, afin de se tenir informée des tendances mondiales et de collaborer avec d'autres autorités de régulation. Cela lui permet d'adapter ses pratiques aux meilleures normes internationales.

5. Accompagnement des entreprises : L'ANPDP offre un accompagnement aux entreprises pour les aider à naviguer dans les complexités légales liées à l'usage des technologies émergentes. Cela inclut des consultations sur les mesures à prendre pour assurer la conformité avec la législation sur la protection des données.

Analyse et Synthèse des Réponses

Synthèse

L’entretien a permis de faire ressortir plusieurs aspects clés du fonctionnement de l’ANPDP et des défis auxquels elle est confrontée. Parmi les principaux défis, on note un besoin accru de sensibilisation des entreprises, notamment des petites et moyennes entreprises, quant à leurs obligations légales en matière de protection des données personnelles. Cette méconnaissance de la loi 18-07, observée dans certains secteurs, complique parfois son application uniforme.

Initiatives et Réalisations Notables

L’entretien a également mis en lumière plusieurs initiatives importantes de l’ANPDP. L'organisation de campagnes de sensibilisation et de formations est perçue comme un outil essentiel pour accompagner les entreprises dans leur mise en conformité. L’autorité développe également des partenariats avec d’autres institutions pour renforcer l’application des mesures de protection des données. Enfin, des outils numériques modernes ont été mis en place pour faciliter le dépôt et le suivi des demandes relatives au traitement des données personnelles. Ces efforts témoignent de l’engagement de l’ANPDP à améliorer ses pratiques et à accompagner les entreprises dans leur démarche de conformité.

Tendances Observées

En résumé, les réponses fournies montrent que l’ANPDP est engagée dans un processus d’amélioration continue, avec un fort accent sur la sensibilisation et la formation des parties prenantes. La collaboration avec les entreprises demeure un axe stratégique pour renforcer la conformité et atteindre les objectifs fixés par la loi 18-07.

Conclusion

Résumé des principaux résultats

L’entretien a permis de mieux comprendre les efforts déployés par l’ANPDP pour promouvoir la conformité à la loi 18-07 et garantir la protection des données personnelles en Algérie. Les initiatives mises en œuvre, telles que les formations, les campagnes de sensibilisation, et les partenariats institutionnels, illustrent un engagement fort en faveur de la régulation et de la sécurité des données personnelles.

Limites de l’entretien

Certaines questions ont reçu des réponses partielles, ce qui nécessitera un suivi avec les responsables de l'ANPDP pour valider les points en suspens.

Conclusion Générale

En conclusion, l’entretien a souligné l’importance cruciale de l’ANPDP dans la régulation de la protection des données personnelles en Algérie. Les efforts entrepris par l’ANPDP pour sensibiliser, former, et accompagner les entreprises dans leur conformité à la loi 18-07 témoignent de son rôle indispensable dans ce domaine.

Annexes

Liste des questions

I. Présentation de l'ANPDP :

1. **Définition et Mission** : Pouvez-vous décrire brièvement l'ANPDP, sa mission principale, et son organigramme ?

2. **Rôles et Responsabilités** : Quels sont les rôles principaux de l'ANPDP pour garantir le respect de la loi 18-07 sur la protection des données personnelles en Algérie ?

3. **Défis Rencontrés :** Quelles sont les principales difficultés rencontrées par l'ANPDP dans l'application de la loi 18-07 depuis son entrée en vigueur ?

II. Conformité Légale et Pratiques :

4. **Exigences pour le Transfert de Données** : Quelles sont les conditions imposées par l'ANPDP pour le transfert de données personnelles à l'étranger, notamment en ce qui concerne l'hébergement sur le cloud ?

5. **Démarches de Conformité** : Quelles étapes clés une entreprise doit-elle suivre pour déclarer et obtenir une licence pour le traitement des données personnelles ?

6. **Ressources disponibles pour la conformité :** Existe-t-il une ‘’ checkliste de conformité ’’ ou un document officiel élaboré par l'ANPDP pour valider les traitements des données a caracters personnelles ?

7. **Impact sur les Entreprises :**Quels défis les entreprises rencontrent-elles lors de la mise en œuvre de la loi 18-07 ?

8. **Améliorations Proposées :** Quelles suggestions l'ANPDP aurait-elle pour améliorer le processus de conformité et aider les entreprises à mieux s'adapter aux exigences de la loi ?

II. Communication et Soutien aux Entreprises :

9. **Mécanismes de Communication** : Quels canaux l'ANPDP utilise-t-elle pour interagir avec les entreprises privées, et quelle est la fréquence de ces échanges ?

10. **Formation et Sensibilisation** : Quels types de formations et de campagnes de sensibilisation l'ANPDP propose-t-elle pour aider les entreprises à se conformer à la loi 18-07 ?

11. **Exemples Concrets** : Pourriez-vous partager des exemples de cas où l'ANPDP a aidé des entreprises à se conformer, ou des cas où des entreprises ont rencontré des difficultés ?

IV. Rôle et Responsabilités :

11. **Rôle du DPO :** Pouvez-vous détailler le rôle et les responsabilités du Délégué à la protection des données (DPO) et ses relations avec l'ANPDP ?

12. **Manuel d'Audit :** L'ANPDP propose-t-elle un manuel ou un cadre type pour aider les entreprises à auditer leur conformité et diagnostiquer leurs processus ?

13. **Processus de nomination des responsables de traitement :** Concernant le processus de nomination des responsables des traitements, est-il possible de disposer d'un modèle officiel de Déclaration d'Honneur , sachant qu'il n'est pas publié sur le site web de 'ANPDP ?

V. Innovations et Perspectives :

14. **Technologies et Sécurité :** Quelles recommandations l'ANPDP fait-elle concernant l'utilisation des technologies de l'information et de la communication (TIC) pour garantir la sécurité et la confidentialité des données personnelles ?

15. **Adaptation aux Technologies Émergentes :** Comment l'ANPDP anticipe-t-elle l'impact des technologies émergentes sur la protection des données personnelles ?

16. **Évaluation de l'Efficacité**: Quels indicateurs l'ANPDP utilise-t-elle pour mesurer l'impact de ses initiatives de sensibilisation auprès des entreprises ?

17. **Coopération Internationale :** Quelles collaborations l'ANPDP entretient-elle avec d'autres autorités de protection des données pour harmoniser les pratiques à l'international ?

VI. Suggestions d'Amélioration :

18. **Retours d'Expérience :** L'ANPDP envisage-t-elle d'ajuster ses méthodes en fonction des retours d'expérience des entreprises sur l'application de la loi ?

19. **Évolution Législative :** Comment l'ANPDP prévoit-elle l'évolution de la législation sur la protection des données pour suivre le développement technologique ?

Documents complémentaires

1. **Loi n° 18-07 du 10 juin 2018** : Relative à la protection des personnes physiques dans le traitement des données à caractère personnel.
2. **Décret présidentiel n° 22-187 du 18 mai 2022** : Fixant la nomination du président et des membres de l'Autorité Nationale de Protection des Données à Caractère Personnel (publié dans le Journal officiel n° 35 de 2022).
3. **Décret présidentiel n° 23-73 du 14 février 2023** : Décrivant les missions, l'organisation et le fonctionnement du secrétariat exécutif de l'Autorité Nationale de Protection des Données à Caractère Personnel (publié dans le Journal officiel n° 10 de 2023).
4. **Décret exécutif n° 24-287 du 22 août 2024** : Fixant les modalités de prise en charge médicale des démunis non-assurés sociaux.
5. **Sites web et ressources utiles** :
    - Site officiel de l'ANPDP : https://anpdp.dz
    - Site officiel du RGPD : https://www.cnil.fr/fr/rgpd
    - Guide sur les bonnes pratiques en matière de confidentialité : https://www.cnil.fr/fr/les-bonnes-pratiques
    - PIA (Privacy Impact Assessment) : https://www.cnil.fr/fr/la-demarche-pia
6. **Documents utilisés pour l'élaboration de ce fichier** :
    - Rapport annuel de l'ANPDP (2023).
    - Guide pratique sur la protection des données personnelles (CNIL, édition 2022).
    - Articles académiques et publications sur la gouvernance des données personnelles et la conformité au RGPD.

Appendix B _ security and personal d

CHARTE DE PROTECTION DES DONNÉES PERSONNEL

Cevital-vers la conformité a la loi 18-07

BENAIDA Meriem

Mbenaida_etd@esgen.edu.dz

1. PRÉAMBULE

La protection des données personnelles est un enjeu majeur dans un environnement numérique en constante évolution. Conformément à la loi algérienne n°18-07 du 10 juin 2018 et aux recommandations de l'Autorité Nationale de Protection des Données à Caractère Personnel (ANPDP), CEVITAL s'engage à assurer la confidentialité et la sécurité des informations personnelles traitées au sein de l'entreprise.

Cette charte a pour objectif de sensibiliser l'ensemble des employés de CEVITAL aux enjeux de la protection des données personnelles et de leur rappeler leurs droits et obligations en la matière.

2. Définitions Officielles

2.1. Loi n°18-07 du 10 juin 2018

La loi n°18-07, promulguée le 10 juin 2018 et publiée dans le Journal Officiel n°34, a pour objet de fixer les règles de protection des personnes physiques dans le traitement des données à caractère personnel en Algérie. Elle a été élaborée dans le cadre de la modernisation de la législation nationale pour se conformer aux standards internationaux en matière de protection de la vie privée. Cette loi s'applique à tous les organismes publics et privés traitant des données personnelles, qu'ils soient établis sur le territoire algérien ou non, dès lors qu'ils utilisent des moyens de traitement situés en Algérie.

2.2. Autorité Nationale de Protection des Données à Caractère Personnel (ANPDP)

L'ANPDP est une autorité administrative indépendante créée en application de la loi n°18-07. Selon le décret présidentiel n°22-187 du 18 mai 2022, l'ANPDP est composée de 15 membres, dont le président, et est chargée de veiller au respect de la loi par le contrôle et la supervision des traitements de données personnelles. Son siège est établi à Alger, et elle joue un rôle crucial dans la délivrance des

autorisations, la réception des déclarations des traitements, ainsi que dans la sanction des manquements .

2.3. Donnée personnelle

Au sens de la loi n°18-07, une donnée personnelle désigne toute information, quel que soit son support, se rapportant à une personne physique identifiée ou identifiable. Par exemple, cela inclut :

- Les informations d'identification (nom, prénom, date et lieu de naissance, numéro de CIN).
- Les coordonnées (adresse, email, numéro de téléphone).
- Les données professionnelles (dossier de recrutement, formation, évaluations).

La définition précise figure à l'article 3 de la loi n°18-07.

2.4. Traitement des données

Le traitement correspond à toute opération ou ensemble d'opérations effectuées sur des données personnelles, que ce soit par des moyens automatisés ou non. Il englobe notamment :

- La collecte
- L'enregistrement
- L'organisation
- La conservation
- La modification
- L'extraction
- La consultation
- L'utilisation
- La diffusion ou la suppression

Ces opérations doivent être réalisées dans le strict respect des principes énoncés par la loi (licéité, transparence, finalité, minimisation, sécurité et conservation limitée).

3. PRINCIPES FONDAMENTAUX DE PROTECTION

Selon l'article 9 de la loi n°18-07 du 10 juin 2018, le traitement des données à caractère personnel doit respecter les principes suivants

3.1. Licéité, transparence et loyauté

- Chaque traitement doit être fondé sur une base légale (consentement exprès, exécution d'un contrat, obligation légale ou intérêt légitime).
- Les personnes concernées doivent être informées de manière claire et accessible de l'identité du responsable, des finalités du traitement et de leurs droits.

3.2. Finalité déterminée, explicite et légitime

- Les données ne sont collectées que pour des finalités précises (ex. gestion RH, relation commerciale) et ne peuvent être utilisées à d'autres fins sans consentement préalable.

3.3. Minimisation, exactitude et conservation limitée

- Seules les données strictement nécessaires sont collectées.
- Les données doivent être exactes et mises à jour (avec des procédures de rectification dans un délai de 10 jours en cas d'erreur).
- La durée de conservation est limitée aux besoins opérationnels ou aux obligations légales (en général entre 5 et 10 ans, sauf exceptions).

3.4. Sécurité et confidentialité

Selon l'article 38, des mesures de sécurité techniques (chiffrement AES 256, authentification multi-facteurs, protocoles SSL/TLS) **et organisationnelles** (contrôle

d'accès, audits semestriels, formations annuelles) **doivent être mises en place pour garantir la protection des données contre tout accès non autorisé, perte ou altération.**

4. MODALITÉS DE COLLECTE, D'UTILISATION ET DE TRAITEMENT

4.1. Catégories de données traitées au sein de cevital

Conformément aux classifications de l'ANPDP et à **l'article 4** de la loi n°18-07, CEVITAL traite plusieurs types de données personnelles en fonction de leur nature et de leur finalité :

- **Données à caractère personnel** : Informations permettant d'identifier une personne, telles que le nom, prénom, date et lieu de naissance, numéro Identifiant National (NIN), coordonnées de contact et documents officiels (CIN, passeport, permis de conduire).
- **Données financières** : Informations relatives aux paiements et transactions, y compris le salaire, le compte bancaire et les primes.
- **Données sensibles** : Informations soumises à une protection stricte, telles que les données de santé, l'appartenance syndicale, les convictions religieuses ou politiques et les données biométriques.
- **Données professionnelles** : Informations liées à l'activité professionnelle des employés, comme le numéro de matricule, le poste occupé, les évaluations, les absences et les formations.
- **Données de connexion et de suivi** : Données collectées pour la sécurité informatique et la gestion des accès, comprenant les adresses IP, les logs de connexion et l'utilisation des outils informatiques.
- **Données de vidéosurveillance et géolocalisation** : Images capturées par les caméras de surveillance et suivi des véhicules de fonction ou équipements professionnels à des fins de sécurité**.**

4.2. Finalités et bases légales

Un traitement de données personnelles ne peut être mis en œuvre que s'il repose sur une finalité clairement définie et une base légale valide. La finalité doit être légitime, explicite et compatible avec la législation en vigueur. Toute utilisation des données en dehors de la finalité initialement déclarée nécessite un consentement supplémentaire ou une justification légale.

▯ Bases légales du traitement des données

Conformément à la loi n°18-07, un traitement de données personnelles doit être justifié par l'une des bases légales suivantes :

- **Consentement explicite de la personne concernée (Article 5)** : lorsque la personne accepte de manière claire et informée que ses données soient collectées et utilisées pour une finalité spécifique.

- **Exécution d'un contrat (Article 6)** : lorsque le traitement est nécessaire pour exécuter un contrat auquel la personne concernée est partie.
- **Obligation légale (Article 7)** : lorsque le traitement est requis pour se conformer à une loi ou une réglementation.
- **Protection des intérêts vitaux de la personne concernée (Article 8)** : lorsque le traitement est nécessaire pour préserver la vie ou la sécurité d'une personne.
- **Exécution d'une mission d'intérêt public (Article 9)** : lorsque le traitement est réalisé pour l'accomplissement d'une tâche relevant de l'intérêt général.
- **Intérêt légitime du responsable du traitement (Article 10)** : lorsque le traitement est justifié par un intérêt légitime de l'entreprise, sous réserve que cet intérêt ne porte pas atteinte aux droits fondamentaux des personnes concernées.

▯ Exemples de finalités de traitement au sein de CEVITAL

- **Gestion des ressources humaines** : traitement des contrats de travail, gestion des paies et des congés (exécution d'un contrat, obligation légale).
- **Sécurité des locaux et des systèmes d'information** : surveillance vidéo, contrôle des accès et gestion des connexions informatiques (intérêt légitime, obligation légale).
- **Gestion des relations commerciales** : facturation, gestion des contrats fournisseurs et clients (exécution d'un contrat, obligation légale).

- **Communication interne et collaboration** : gestion des comptes email professionnels et des plateformes collaboratives (intérêt légitime).

Ces finalités doivent être déclarées et respectées scrupuleusement pour garantir la conformité avec la loi 18-07 et assurer la protection des droits des personnes concernées.

4.3. Mesures techniques et organisationnelles

Pour garantir la sécurité des données personnelles traitées, CEVITAL met en place les mesures suivantes :

- **Contrôle des accès** : Seules les personnes autorisées ont accès aux informations sensibles, selon leur rôle et leurs responsabilités.
- **Chiffrement et anonymisation** : Les données sensibles sont protégées par des mécanismes de chiffrement et d'anonymisation lorsque cela est nécessaire.
- **Surveillance et audits** : Des audits de sécurité sont réalisés régulièrement pour détecter et corriger toute faille de sécurité.
- **Sensibilisation et formation** : Des formations régulières sont dispensées aux employés pour garantir une bonne compréhension des règles de protection des données.

5 DROITS DES PERSONNES CONCERNÉES

Une personne concernée désigne toute personne physique dont les données personnelles sont collectées, stockées ou traitées dans le cadre des activités de CEVITAL. Il peut s'agir :

- Des employés et collaborateurs internes.
- Des candidats à un emploi.
- Des clients et fournisseurs.
- Des visiteurs des locaux de l'entreprise.
- De toute autre personne dont les données sont traitées par CEVITAL dans le cadre de ses activités.

Conformément aux **articles 32 à 36** de la loi 18-07, les personnes concernées disposent des droits suivants :

- **Droit à l'information (Article 32)** : Toute personne a le droit d'être informée de manière claire et transparente sur les traitements de ses données personnelles, la finalité du traitement et les destinataires de ces données.
- **Droit d'accès (Article 33)** : Toute personne peut demander à consulter ses données personnelles détenues par CEVITAL et obtenir des informations sur les traitements effectués.
- **Droit de rectification (Article 34)** : En cas d'inexactitude ou de modification de ses données, la personne concernée peut demander leur correction ou leur mise à jour.
- **Droit d'opposition (Article 35)** : Toute personne peut s'opposer au traitement de ses données personnelles pour des motifs légitimes, sauf en cas d'obligation légale contraire.

Les demandes relatives aux droits mentionnés ci-dessus doivent être adressées au **Délégué à la Protection des Données (DPO)** de CEVITAL. Toute demande doit être accompagnée d'un justificatif d'identité et sera traitée dans un délai raisonnable conformément aux dispositions légales.

5. Sanctions en cas de non-conformité

Le non-respect des obligations relatives à la protection des données personnelles peut entraîner des sanctions légales et disciplinaires. La loi n°18-07 prévoit des mesures strictes pour toute violation des règles de traitement des données personnelles.

5.1. Sanctions légales

Conformément aux dispositions de la **loi n°18-07**, toute infraction aux règles de protection des données personnelles peut donner lieu à des sanctions administratives, civiles et pénales :

- **Infractions générales** : Toute collecte, traitement ou conservation de données personnelles en violation des principes établis par la loi peut être sanctionnée par **des amendes pouvant atteindre 500 000 DA** et des injonctions de mise en conformité émises par l'ANPDP.
- **Divulgation non autorisée** : La divulgation, intentionnelle ou non, de données personnelles sans consentement ou sans base légale appropriée peut entraîner **des peines d'emprisonnement allant jusqu'à 5 ans** et des sanctions financières.
- **Traitement illicite de données sensibles** : Le traitement de données sensibles (santé, origine raciale, opinions politiques, etc.) sans autorisation spécifique est puni **d'une amende et d'une interdiction d'exercer certaines activités**.
- **Transfert non autorisé de données vers un pays tiers** : Tout transfert de données hors du territoire national sans autorisation préalable est strictement interdit et peut être passible **de lourdes amendes et de sanctions pénales**.

L'**Autorité Nationale de Protection des Données à Caractère Personnel (ANPDP)** est responsable de la surveillance et du contrôle du respect de la loi 18-07. Elle peut exiger des audits, ordonner la suspension d'un traitement de données et infliger des sanctions administratives.

5.2. Sanctions internes chez CEVITAL

En plus des sanctions prévues par la loi, CEVITAL applique des **sanctions disciplinaires internes** en cas de non-respect des règl\es de protection des données :

- **Avertissement ou blâme** en cas de négligence dans l'application des politiques internes.
- **Suspension temporaire des accès aux systèmes informatiques** en cas de violation de la confidentialité des données.
- **Sanctions disciplinaires pouvant aller jusqu'au licenciement** en cas de faute grave, notamment en cas de divulgation non autorisée, de falsification de données ou d'accès illégal aux systèmes d'information.

Appendix C _ awareness poster

Appendix D_ Simulation of the ANPDP Declaration Forms

Information sur le traitement DPO															
Champ / Élément	Traitement 1	Traitement 2	Traitement 3	Traitement 4	Traitement 5	Traitement 6	Traitement 7	Traitement 8	Traitement 9	Traitement 10	Traitement 11	Traitement 12	Traitement 13	Traitement 14	Tra nt
Dénomination du traitement mis en place	Administration du Personnel	Gestion Mutuelle Santé	Traitement de la Paie	Gestion de la formation	Gestion des apprentis	Gestion des stagiaires	Collecte et traitement de CV et candidatures	Gestion des entretiens (Physique, Téléphonique, Videoconférence)	Vérification des références (Candidats)	Révisions salariales	Reporting RH	Gestion de la performance	Gestion des newsletters et communication internes	Campagnes marque employeur Linked In	Méde du trav
Type du traitement	Manuel / Automatique	Automatique	Automatique	Manuel	Manuel	Manuel	Manuel / Automatique	Manuel / Automatique	Manuel / Automatique	Automatique	Automatique	Automatique	Automatique	Automatique	Manu
Finalité (but) du traitement	Structurer, organiser et gérer toutes les activités liées à la gestion administrative du personnel, tout en garantissant le respect des	Fournir une couverture complémentaire aux salariés afin de compléter les remboursements des frais de santé et d'assurance décès.	Gérer et calculer les salaires des employés conformément aux lois et réglementations en vigueur.	Développer les compétences des employés, améliorer la performance de l'entreprise et garantir la conformité avec les obligations légales et	Assurer le suivi de la formation des apprentis et leur développement professionnel au sein de l' entreprise, tout en garantissant la conformité avec les exigences légales et	Assurer le suivi de la performance des stagiaires pour faciliter leur insertion professionnelle future, tout en veillant au respect des obligations	Traitement et évaluation des candidatures en vue de pourvoir les postes vacants.	Évaluation des compétences et vérification de l'adéquation du profil du candidat au poste à pourvoir.	Vérification de l'exactitude des informations fournies par le candidat	Application de la politique salariale du Groupe	Fournir des informations pertinentes et précises pour aider la direction à gérer efficacement ces ressources humaines	Gestion des évaluations annuelles	Informer les employés des actualités	Promouvoir l'image employeur	Prés r et prom ir l sant des trav eurs dans cadr leur acti prof onne

	règles légales et internes.			réglementaires en matière de formation professionnelle.	réglementaires	administratives									
Cadre légal du traitement	* Consentement * Obligation légale * Exécution d'un contrat	* Consentement * Exécution d'un contrat (Convention)	* Obligation légale	*Consentement * obligation légale * exécution d'un contrat *Intérêt légitime	*Consentement * obligation légale * exécution d'un contrat *Intérêt légitime	*Consentement * exécution d'un contrat *Intérêt légitime	* Consentement	* Consentement	* Intérêt légitime	* Intérêt légitime	* intérêt légitime	* Consentement * Exécution d'un contrat	* Consentement	* Intérêt légitime	* Obligation légale
Nom et Prenom du contrat (point focal)	Amine CHERIGUI	Feriel BOUDAH	Dalila AGGOUNE	Amina Haif	Amina Haif	Amina Haif	Ouafa BIAZ	Ouafa BIAZ	Ouafa BIAZ	Amrane ZOUAGUI	ABADA Mohamed	Soumia LADJEROUD	Mohamed Bachir KRIMAT	Mohamed Bachir KRIMAT	Amine CHERIGUI

Qualité	Chargé Gestion Administrative	Chargé Gestion Administrative	Responsable Paie & Personnel Etranger Groupe	Responsable Formation Groupe	Responsable Formation Groupe	Responsable Formation Groupe	Responsable Recrutement	Responsable Recrutement	Responsable Recrutement	Directeur Rémunération & Performance	Responsable pilotage RH	Manager Transformation et processus RH	Responsable Marque Employeur	Responsable Marque Employeur	Chargé Gestion Administrati
Service	DRHG	DRHG	DRHG	Formation	Formation	Formation	Recrutement / DRH	Recrutement / DRH	Recrutement / DRH	DRHG	DRHG	DRHG	DRHG	DRHG	DRHG
Indiquez les catégories des traitements	* Gestion du Personnel	* Gestion des Adhérents	* Gestion de la paie	*Gestion du personnel * Gestion des Fournisseurs	* Gestion des Étudiants/ Élèves.	* Gestion des Étudiants/Élèves.	* Gestion des candidatures	* Gestion des candidatures	* Gestion des candidatures	* Gestion du Personnel	* Gestion du Personnel	* Gestion du Personnel	* Communication	* Communication	* Gestion du Personnel
Existence des sous-traitements	oui	Non	Non	Non	Non	Non	Oui	Non	Non	Non	Non	Non	Non	Non	Non

Données collectées															
Champ / Élément	Traitement 1	Traitement 2	Traitement 3	Traitement 4	Traitement 5	Traitement 6	Traitement 7	Traitement 8	Traitement 9	Traitement 10	Traitement 11	Traitement 12	Traitement 13	Traitement 14	Tr
Type de collecte de données	Manuel / Automatique	Manuel / Automatique	Manuel / Automatique	Manuel	Manuel	Manuel	Manuel / Automatique	Manuel/Automatique	Automatique	Automatique	Manuel	Manuel / Automatique	Manuel	Manuel	Ma

Mode de collecte	* Intranet * Poste déconnecté * Papier	* Intrenet * Poste déconnecté	* Intranet	* Poste déconnecté * Intranet * Internet	* Poste déconnecté * Intranet * Internet	* Poste déconnecté * Intranet * Internet	* Poste déconnecté * Interanet * Internet	* Poste déconnecté * Internet	* Poste déconnecté	* Intranet	* Intranet	* Poste déconnecté * Intranet * Internet	* Intranet * Internet	* Internet * Appareil Photo	* Pa
La sécurité de la collecte des données	* Traçabilité	* Traçabilité	* Traçabilité	* Traçabilité	* Traçabilité	* Traçabilité	* Traçabilité * Charte de sécurité	* Traçabilité * Charte de sécurité	* Traçabilité	* Traçabilité	*Traçabilité	* Traçabilité	* Tracabilité	* Tracabilité	* Tr li
Indiquez les cotégories des personnes concerneés	* Salariés	*Adhérent et ayants droit au sens de la sécurité sociale	* Salariés	* Fournisseurs * Salaries	* Etudiants/Élèves	* Etudiants/Élèves	*Candidats	*Candidats	Candidats	*Salariés	*Salaries	* Salaries	*Salariés	*Grand public	* Sa s
Avez-vous d`autre sousrce de données utiliséesdans la collec	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	No

te des données														
Nom (BD) ou (FM)	SAP/Portail RH/CREDOID	Plateforme RH	SAP/SAGE/CREDOID	Fichier manuel Outlook	Fichier manuel Outlook	Fichier manuel Outlook	BD/ LinkedIn Archive recrutement	Dossier du candidat	Dossier du candidat	/	SAP, SAGE, Fichier Excel	FM	Filiales	Filiales
Nom structure propriétaire	DRH	DRH	DRH	DRH	DRH	DRH	Recrutement	Recrutement	Recrutement	/	DRHG	DRHG	DRHG	DRHG
Moyen de collecte	* Papier * Support externe * Connexion	* Papier * Support externe * Connexion	* Papier * Connexion	* Papier *Connexion	* Papier *Connexion	* Papier *Connexion	* Papier * Connexion	* Entretien face to face * Téléphone * Connexion	* Téléphone * Connexion	/	Connexion	* Papier * Connexion	* Connexion	* Connexion
Objectifs	Gestion du personnel et pointage	Prise en charge des soins médicaux + garanties décès et invalidité	Établir la paie et procéder à son virement.	Gestion et suivi des formations des collaborateurs.	Gestion et suivi des apprentis	Gestion et suivi des stagiaires	Pourvoir des postes vacants	Evaluation des compétences et vérification de l'adéquation du profil du candidat au poste à pourvoir	Vérifier l'exactitude des informations fournies par le candidat	/	Fournir des informations RH pertinentes et précises	gestion des objectifs evaluation de la performance	amélioration de la communication interne	développement de la mraque employeur

Catégorie des données collectées et traitées															
Champ / Élément	Traitement 1	Traitement 2	Traitement 3	Traitement 4	Traitement 5	Traitement 6	Traitement 7	Traitement 8	Traitement 9	Traitement 10	Traitement 11	Traitement 12	Traitement 13	Traitement 14	Tra nt

Catégorie	* Données à caractère Personnel * Données à caractère Professionnelles * Données sensibles	* Données à caractère Personnel * Données Sensibles	* Données à caractère Personnel * Données à caractère Professionnelles * Données financières	* Données à caractère personnel * Données professionnelles * Données financières * données sensibles	* Données à caractère personnel * Données professionnelles * Données financières * Données sensibles	* Données à caractère personnel * Données professionnelles * Données sensibles	* Données à caractère personnel * Données professionnelles * Données financières	* Données à caractère personnel * Données professionnelles * Données financières	* Données à caractère personnel * Données professionnelles	* Données à caractère personnel * Données professionnelles * Données financières	* Données à caractère personnel * Données professionnelles	*Données à caractères personnel *Donneés profesionnelles	*Données à caractères personnel *Données profesionnelles	* Donn à cara e Pers l * Donn à cara e Prof onne * Donn sens s

Type d`informations recueillies	Données à caractère Personnel : * N° Identifiant National (NIN) * N° Sécurité Sociale * Nom et Prénom * Date de Naissance * Lieu de Naissance * Situation familiale * Photo * Adresse du domicile * Adresse Mail * N° de téléphone * Nom et Prénom (Conjoint/Enfants) * Date de Naissance (Conjoint/Enfants) * Lieu de Naissance (Conjoint/Enfants) * Situation au Service National * Permis de conduire * Diplôme * Certificat de	Données à caractère Personnel : * Nom et Prénom * Date de naissance * Situation Familiale * Nom et Prénom (Conjoint + Enfants) * Date de naissance (Conjoint + Enfants) * Adresse mail	Données à caractère Personnel : * Nom et Prénom * Date de Naissance * Lieu de Naissance * Situation familiale * Adresse du domicile * Nombre d'enfants scolarisés	Données à caractère Personnel : * Nom et Prénom * Date de Naissance * Photo * Adresse Mail * N° de téléphone	Données à caractère Personnel : *Nom et Prénom * Date de Naissance * Adresse du domicile * Adresse Mail * N° de téléphone * N° de la pièce d'identité	Données à caractère Personnel : *Nom et Prénom * Date de Naissance * Adresse du domicile * Adresse Mail * N° de téléphone * N° de la pièce d'identité	Données à caractère personnel : * Nom & prénom * Date de naissance * Lieu de naissance * Situation familiale * Adresse du domicile * Adresse mail * N° de téléphone * Situation vis-à-vis du SN * Niveau d'étude	Données à caractère personnel : * Nom & prénom *Date de naissance *Lieu de naissance * Situation familiale *Adresse du domicile * Adresse mail * N° de téléphone * Situation vis-à-vis du SN * Niveau d'étude * Diplôme	Données à caractère personnel : * Nom et Prénom * Adresse Mail	Données à caractère personnel : * Nom et Prénom * Date de Naissance * Sexe	Données à caractère personnel : * Nom et Prénom	Données à caractère personnel : * Nom et prénom * Photo * Adresse mail * Numéro de téléphone	Données à caractère personnel : * Nom et prénom * Photo * Témoignages	Donn à cara e Pers l : * No Prén * Da de Nais e * Li de Nais e * Situ n fami e

travail (ancien employeur) * Casier judiciaire * Numéro de Passeport (Expatrié)					* Diplôme			
Données financières : * Revenu * Compte bancaire * Elements de rémunération(SB/CANS/IRG...)	Données financières : * Remboursement des soins de santé	Données financières : * Revenu * Compte bancaire * Elements de rémunération	Données financières : *Contrat de fidélité *Rétribution du formateur interne	Données financières : * Revenus * Compte bancaire *Prime maitre d'apprentissage	Données financières : * Salaire actuel * Salaire souhaité	Données financières : * Salaire actuel * Salaire souhaité	Données financières : * Salaire de base * Primes et indemnités	* Données financières : * Revenu * Eléments de paie

Données sensibles : * Empreinte biométrique * Groupage sanguin * Certificat Phtisio et Général * Sérologie (Expatrié)	Données sensibles : * Actes médicaux	Données sensibles : *Données de santé	Données sensibles : *Données de santé	Données sensibles : *Données de santé										Donn sens s : * Info ions médi s * Grou sang * Anté nts médi * Résu s de test alys
Données professionnelles : * Matricule * Date de recrutement * Direction/Fonction * Responsable hiérarchique * Date de départ * Raison du départ * Pointage (Absences) * N° de téléphone Pro	Données professionnelles : * Date de recrutement * Date de départ	Données professionnelles : * Matricule * Date de recrutement * Direction/Fonction * Date de départ	Données professionnelles : *poste occupé *Structure et direction d'appartenance *Registre de Commerce *Statut *Agrément	Données professionnelles : *Centre de formation professionnel (nom, prénom) *Diplôme préparé	Données professionnelles : * Ecoles/Universités * Diplôme préparé	Données professionnelles : * Poste actuel * Postes antérieurs	Données professionnelles : * Poste actuel * Postes antérieurs * Durée du préavis	Données professionnelles : * Poste actuel * Postes antérieurs * Raisons de départ	Données professionnelles : * Matricule pro * Date d'embauche * Fonction * Structure de rattachement	Données professionnelles : - Matricule - Entité - Date de recrutement - Type de contrat - Poste/Direction/Département - Catégorie Socio-professionnelle - Formation (intitulé/date/durée/coût)	Données professionnelles : - Mail - N° de téléphone Pro - Matricule - Date d'intégration - Entreprise - Poste occupé -	Données professionnelles : - Numéro Adresse mail - Matricule - Poste - Direction de ratachement - Filiale	Données professionnelles : - Fonctions	Donn profe onne : * Matr e * Da de recr ent * Dire n/Fo on

	* Adresse Mail Pro		* Pointage (Absences)							- Accident du travail (date/durée/cause) - Absence (type/date/durée) - Date de départ - Type de départ	Direction de rattachement			
Origine de la donnée	* Pers concernée * Autre	* Pers concernée	* Pers concernée * Autre	* Pers concernée * Autre	* Pers concernée * Autre	* Pers concernée * Autre	* Pers concernée	* Pers concernée	* Autre	* Autre	* Autre	* Autre	* Pers concernée * Autre	* Autre	* Pe conc e * Au
Sources de données	* Formulaire * Dossiers Papiers * Base de données	* Formulaire * Dossiers Papiers	* Dossiers Papiers * Base de données	* Formulaire * Dossiers papiers * Base de données	* Formulaire * Dossiers papiers * Base de données	* Formulaire * Dossiers papiers * Base de données	* Formulaire * Dossiers papiers * Base de données * Autre	* Formulaire * Entretien d'embauche * Entretien Téléphonique * Entretien vidéo-conférence	*Anciens employeurs *Anciens Managers du candidat	* Fichier Excel	*Base de données / Excel	* Formulaire	* Formulaire * Base de données * Prise photos	* Prise de photos	* Form re * Doss Papi

Durée de conservation	Limité	Limité	Limité	Limitée	Limitée	Limitée	Limitée	Limitée	Limitée	Limitée	Limité	Limitée	Limitée	Illimité	Limi
Préciser la durée ?	10 ans après la fin de la relation de travail	1 An	10 ans après la fin de la relation de travail	5 ans après la fin de la relation de travail	5 ans après la fin de la relation de travail	5 ans après la fin de la relation de travail	24 mois	24 mois	24 mois	5 ans	10 ans après la fin de la relation de travail	5 ans après la fin de la relation de travail	10 ans		10 aprè fin la rela de trav

conservation des données															
Champ / Élément	Traitement 1	Traitement 2	Traitement 3	Traitement 4	Traitement 5	Traitement 6	Traitement 7	Traitement 8	Traitement 9	Traitement 10	Traitement 11	Traitement 12	Traitement 13	Traitement 14	Tr en
Comment les données sont elles conservées	Manuel / Informatique	Manuel / Informatique	Manuel / Informatique	Manuel / Informatique	Manuel / Informatique	Manuel / Informatique	Manuel / Informatique	Manuel / Informatique	Manuel	Informatique	Informatique	Informatique	Informatique	Informatique	Ma

conservation des données manuel et informatique															
Champ / Élément	Traitement 1	Traitement 2	Traitement 3	Traitement 4	Traitement 5	Traitement 6	Traitement 7	Traitement 8	Traitement 9	Traitement 10	Traitement 11	Traitement 12	Traitement 13	Traitement 14	Tr en
Nom de la base de données	SAP/SAGE/CREDOID/ Portail RH/Excel	Platforme Mutuelle santé	SAP/SAGE/Excel	Fichier de partage one drive	Fichier de partage one drive	Fichier de partage one drive	Partage DRH Groupe	Partage DRH Groupe	Partage DRH Groupe	Ficher Excel	Excel Reporting	SAP SUCCESS FACTORS	Excel (BD communication)	linkedin, Cloud (one drive)	
Lieu de stockage de la base de données	Serveur	AGLIC (Sous-traitant)	Serveur	Cloud	Cloud	Cloud	Partage DRH	Partage DRH	Partage DRH	PC professionnel	PC	Cloud	PC pro		

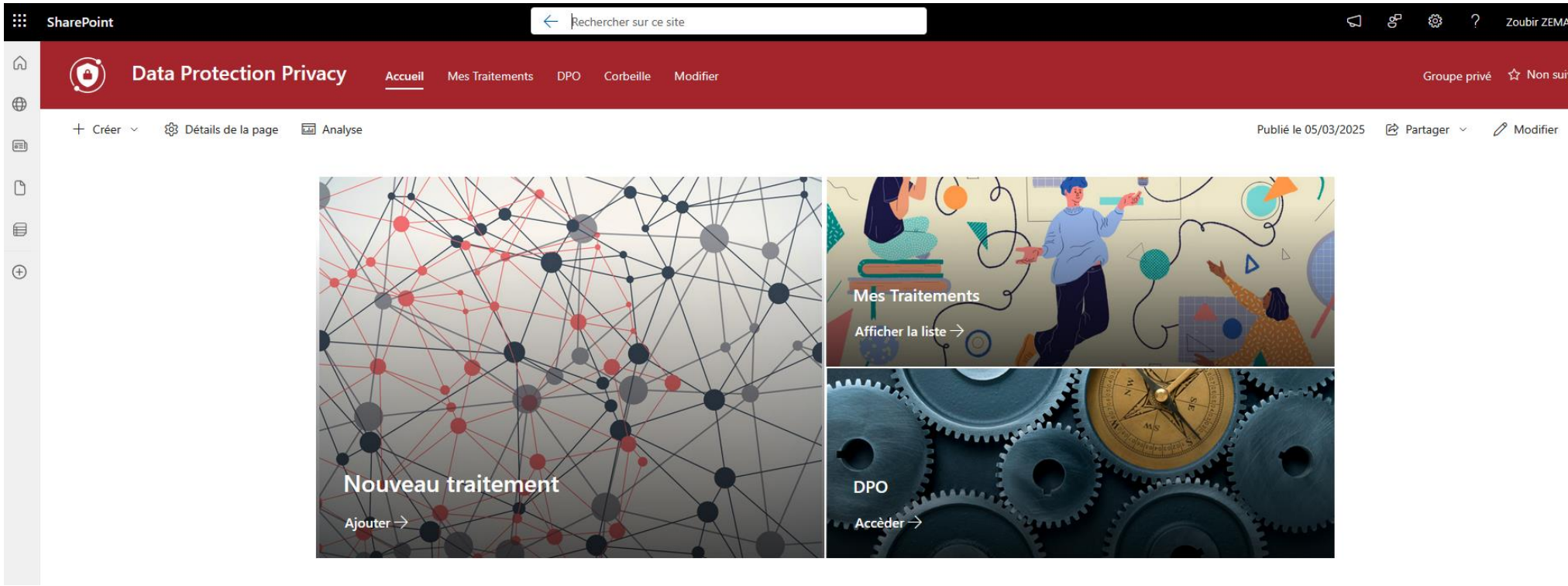
Cadre légal	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	/
Nom du fichier manuel	Dossiers salariés		Livre de Paie	1- Chrono Formation 2- Chrono bon de commande	1- Chrono Dossier administratif	1-Chrono Stagiaires 2- Rapports de stage	Archive Recrutement	Archive Recrutement	Archive Recrutement					Dos mé x
Lieu des sockage du fishier	DRH		DRH	DRH	DRH	DRH	DRH	DRH	DRH					DR
Cadre légal	Conformité à la loi 18-07		Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07	Conformité à la loi 18-07					Co it la 18

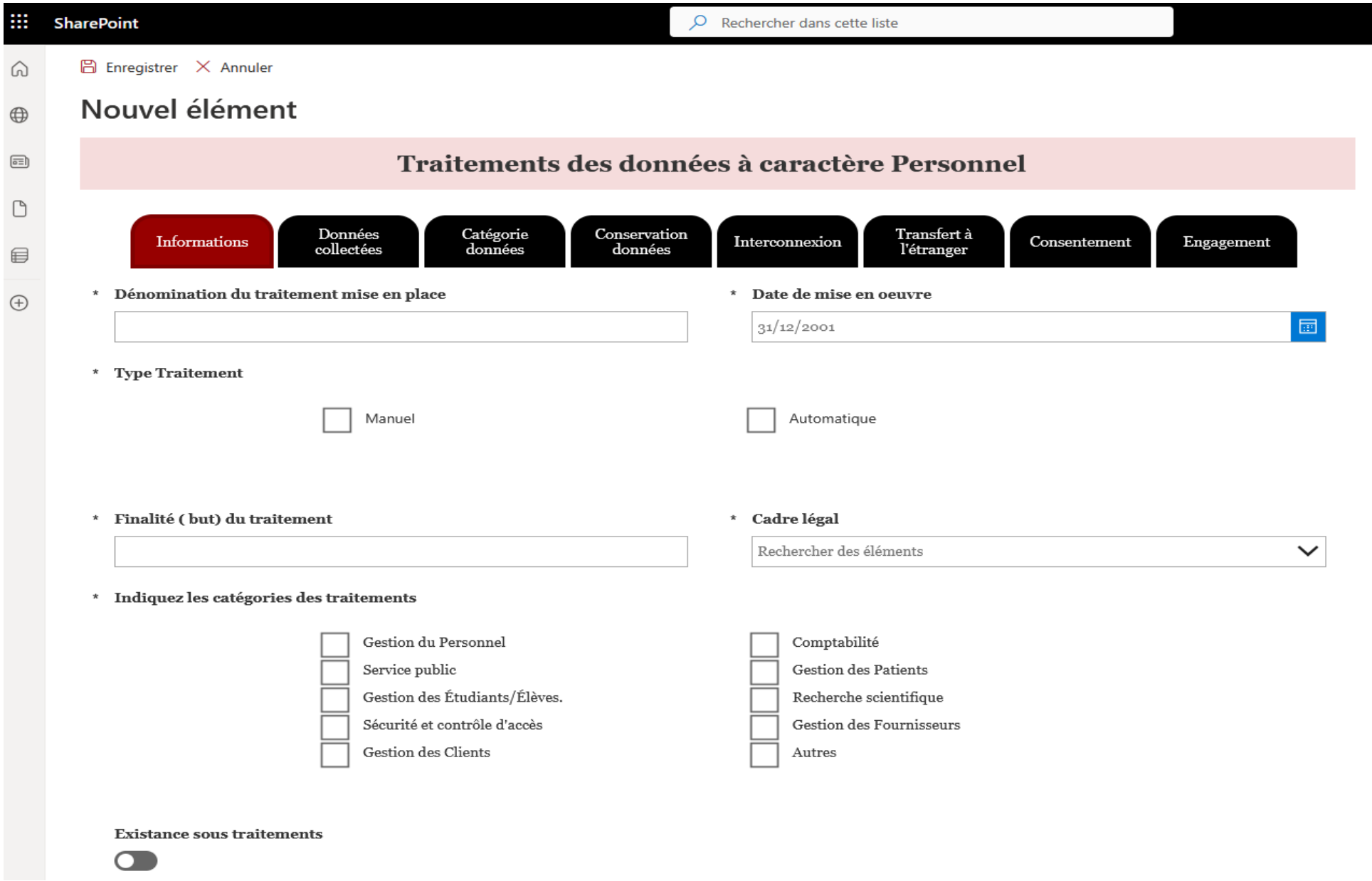
Interconnexion et/ou communication des données collectées à des tiers														
Champ / Élément	Traitement 1	Traitement 2	Traitement 3	Traitement 4	Traitement 5	Traitement 6	Traitement 7	Traitement 8	Traitement 9	Traitement 10	Traitement 11	Traitement 12	Traitement 13	Traitement 14	Tr en
Est-ce que vous communiquez des données à caractere personnel à des tiers ou avez des interconnexions	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non	Non	Oui	Oui	Ou
si oui															

Nom de l'organisme destinataire	CNAS / Impôts / Inspection du Travail / Direction de l'emploi	Algérienne Vie	CNAS / Impôts /Banque	*Centres de formation *hôtels *formateurs *Filiales Cevital	*Centres de formation professionnels *Filiales Cevital	*Ecoles / universités *Filiales Cevital				Filiales du Groupe	Reseaux sociaux	La oi d' se
Mode de communication	* Papier * Connexion	Connexion	* Papier * Connexion	* Papier * Connexion	* Papier * Connexion	* Papier * Connexion				* Connexion * Papier	* Connexion	* Ec ll d' se
Objectifs	Obligation légale	Convention	Obligation légale	*Prestation de service *Gestion de la formation des collaborateurs	Encadrement des apprentis	Encadrement des stagiaires				Information Communication	Partage pour développement de l'image de marque	Di ti mé

Cadre légal	* Loi n° 90-11 du 21 avril 1990 relative aux relations de travail *Loi n° 81-10 du 11 juillet 1981 relative aux conditions d' emploi des travailleurs étrangers	Convention	* Loi n° 90-11 du 21 avril 1990 relative aux relations de travail	* Loi n° 90-11 du 21 avril 1990 relative aux relations de travail	* Loi n° 90-11 du 21 avril 1990 relative aux relations de travail * Loi n° 08-04 du 23 juin 2008	* Loi n° 90-11 du 21 avril 1990 relative aux relations de travail * Loi n° 08-04 du 23 juin 2008	Conformité à la loi 18-07	Conformité à la loi 18-07	* n° 11 21 av 19 re e re ns tr

Appendix E _ Internal Collection Platform (SharePoint)




SharePoint
Rechercher dans cette liste
Enregistrer
Annuler
Nouvel élément
Traitements des données à caractère Personnel
Informations
Données collectées
Catégorie données
Conservation données
Interconnexion
Transfert à l'étranger
Consentement
Engagement
* Dénomination du traitement mise en place
* Date de mise en oeuvre
31/12/2001
* Type Traitement
Manuel
Automatique
* Finalité (but) du traitement
* Cadre légal
Rechercher des éléments
* Indiquez les catégories des traitements
Gestion du Personnel
Service public
Gestion des Étudiants/Élèves.
Sécurité et contrôle d'accès
Gestion des Clients
Comptabilité
Gestion des Patients
Recherche scientifique
Gestion des Fournisseurs
Autres
Existance sous traitements

Enregistrer Annuler

Nouvel élément

Traitements des données à caractère Personnel

Informations | Données collectées | Catégorie données | Conservation données | Interconnexion | Transfert à l'étranger | Consentement | Engagement

Mode de collecte

◯ Poste déconnecté ◯ Intranet ◯ Internet

La sécurité de la collecte des données :

☐ Traçabilité
☐ Signature électronique
☐ Chiffrement
☐ Charte de sécurité

Indiquez les catégories des personnes concernées :

☐ Adhérant
☐ Salaries
☐ Patients
☐ Etudiants/Élèves
☐ Fournisseurs
☐ Usagés
☐ Clients (actuels ou potentiels)
☐ Autres

Autres Sources

Type Collecte

☐ Manuel
☐ Informatique

Enregistrer Annuler

Nouvel élément

Traitements des données à caractère Personnel

Informations | Données collectées | Catégorie données | Conservation données | Interconnexion | Transfert à l'étranger | Consentement | Engagement

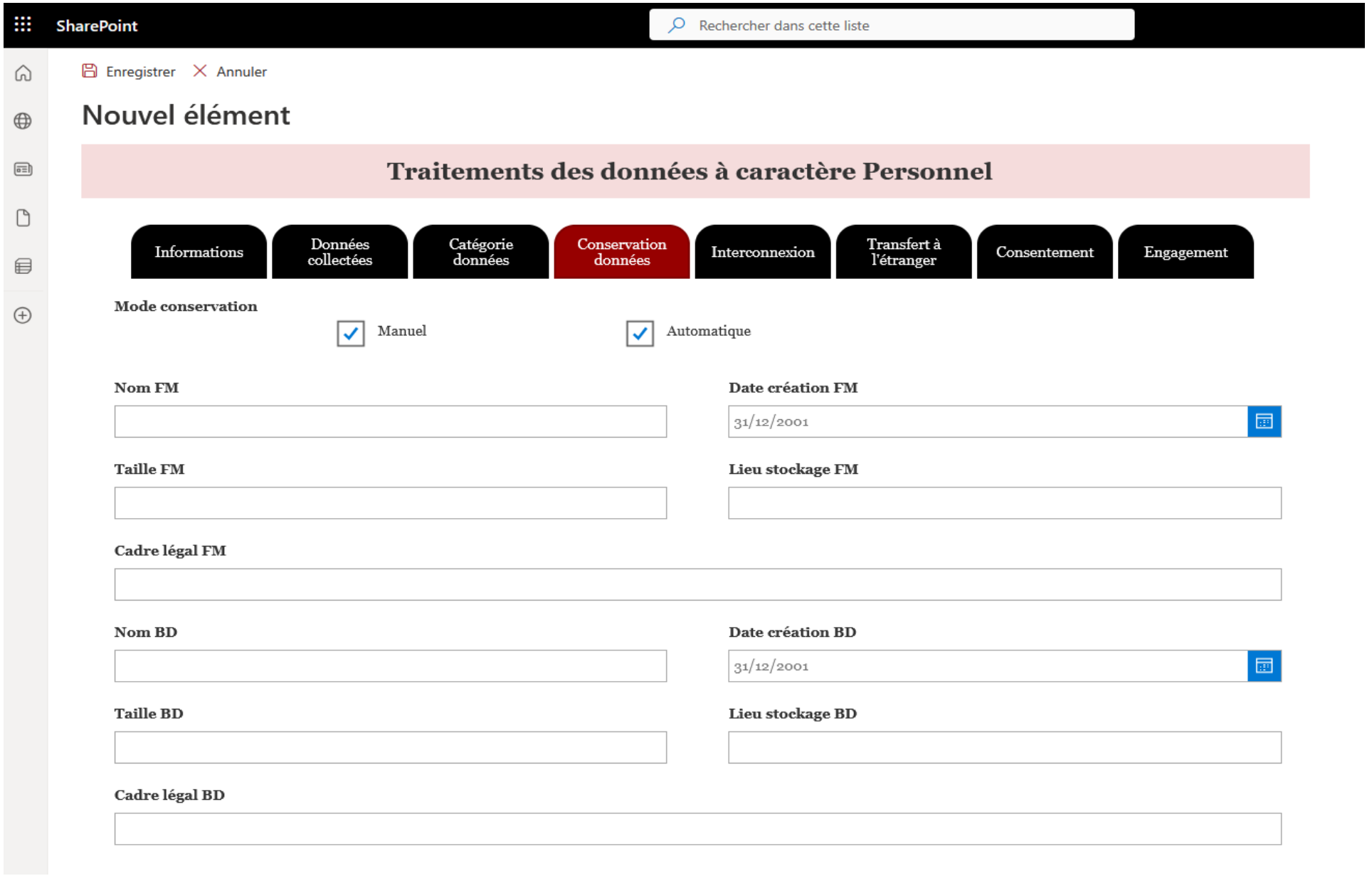
Catégories Données

Rechercher des éléments

Type Informations

Rechercher des éléments

Conservation Limitée


SharePoint
Rechercher dans cette liste
Enregistrer
Annuler
Nouvel élément
Traitements des données à caractère Personnel
Informations
Données collectées
Catégorie données
Conservation données
Interconnexion
Transfert à l'étranger
Consentement
Engagement
Mode conservation
Manuel
Automatique
Nom FM
Date création FM
31/12/2001
Taille FM
Lieu stockage FM
Cadre légal FM
Nom BD
Date création BD
31/12/2001
Taille BD
Lieu stockage BD
Cadre légal BD

Enregistrer Annuler

Nouvel élément

Traitements des données à caractère Personnel

Informations | Données collectées | Catégorie données | Conservation données | Interconnexion | Transfert à l'étranger | Consentement | Engagement

Est-ce que vous communiquez des données à caractere personnel à des tiers ou avez des interconnexions ?

Nom organisme destinataire

Objectifs communication

Cadre légal communication

Mode Communication

Rechercher des éléments

Enregistrer Annuler

Nouvel élément

Traitements des données à caractère Personnel

Informations | Données collectées | Catégorie données | Conservation données | Interconnexion | Transfert à l'étranger | Consentement | Engagement

Consentement des personnes concernées : existe-il ?

Indiquer la methode de consentement

Enregistrer Annuler

Nouvel élément

Traitements des données à caractère Personnel

Informations | Données collectées | Catégorie données | Conservation données | Interconnexion | Transfert à l'étranger | Consentement | Engagement

* **Je m'engage à effectuer le traitement conformément aux dispositions de la loi n° 07-18 du 10 juin 2018, relative à la protection des personnes physiques en matière de Traitement de données à caractère personnel** ☑

* **Je m'engage à informer, sans délais, DPO de chaque modification qui survient sur les informations déclarées et aussi de la suppression du traitement.** ☑

* **Je déclare sur l`honneur que les renseignements, objet de cette déclaration, sont véridiques, complets, exacts et respectent les exigences de la législation en matière de projection des données à caractère personnel.** ☑