Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.11 n.52, p. 148-155. March./April., 2025.
DOI: https://doi.org/10.5935/jetia. v11i52.1556

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

A TAILORED COMPLIANCE SOLUTION FOR SECURING PERSONAL DATA PRIVACY UNDER LAW 18-07 IN ALGERIA

Redouane Guettal [1], Mohammed Kamel Benkaddour [2]

[1] Department of Computer Science and Information Technology, Kasdi Merbah University, Ouargla, Algeria.
[2] Department of Computer Science and Information Technology, Laboratory of Artificial Intelligence and Information Technologies (LINATI), Kasdi Merbah University, Ouargla, Algeria.

[1] http://orcid.org/0009-0006-2471-3242, [2] https://orcid.org/0000-0003-1895-7540

Email: Guetta.redou1@gmail.com, Benkaddour.kamel@univ-ouargla.dz

ARTICLE INFO

Article History
Received: January 12, 2025
Revised: January 20, 2025
Accepted: March 15, 2025
Published: April 30, 2025

Keywords:
Data security,
Personal data privacy,
Processing of personal data,
Law 18-07, ANPDP.

ABSTRACT

In an increasingly digitalized world, the management and protection of personal data has become a crucial issue for companies and governments. The rapid flow of information and the ubiquity of technology pose significant challenges to data security and privacy. In response to these concerns, the Algerian state enacted Law 18-07 on June 10, 2018, aimed at protecting individuals concerning the processing of their data. This law led to the creation of the National Authority for the Protection of Personal Data (ANPDP), responsible for supervising its application. This article proposes the design and implementation of a computer application dedicated to compliance with Law 18-07 for the protection of personal data. We first collected and analyzed the legal requirements for data protection and then modeled them using UML diagrams following the UP methodology. We have set up a database management system to ensure data protection and optimized management, incorporating cryptography techniques to enhance the security of the information. The development of this application was carried out with the Microsoft Visual FoxPro V.9 language, thus allowing the creation of a database and interfaces adapted to the needs of algerian companies to comply with Law 18-07 and guarantee the security of personal data.

I. INTRODUCTION

With the increasing spread of personal data around the world, growing concerns emerge regarding the protection of individuals' privacy and trust in computer systems. The ubiquity of personal data and its rapid flow across borders, in a world where technology pervades all domains, raises major concerns about preserving individual privacy and trust in IT systems. Compliance with data protection laws thus becomes an imperative necessity to ensure assurance and security in technological environments, where personal data is collected, stored, and shared at an unprecedented rate [1].

Algeria's adoption of Law 18-07 in 2018 marks a significant step forward in the protection of personal data. This law, inspired by international standards, regulates the collection, processing, and use of personal data by organizations. It plays a crucial role in building trust between consumers and service providers, which is essential for boosting digital economies. However, compliance with this law presents technical and organizational challenges that companies face [1], [2].

Algerian companies face many obstacles in applying Law 18-07, including the understanding the legal requirements, which are often complex, making compliance difficult. Implementing technical and organizational measures to protect personal data, which requires significant resources. Managing individuals' rights, such as access, rectification, or opposition to the processing of their data. Identifying and correcting flaws in existing IT systems, which are not always adapted to current legislation and the risks related to non-compliance, which may result in legal sanctions or reputational damage [2].

This article proposes the design and implementation of a computer application dedicated to compliance with Law 18-07. Its aim is to provide companies with a practical and accessible tool for complying with legal data protection requirements while strengthening the security and efficient management of their IT systems.

II. RESEARCH BACKGROUND

II.1 PRIVACY AND PERSONAL DATA

Privacy is the right of an individual to determine when, how, and to what extent that information is shared with others, as defined by [3]. According to [4], the concept of personal data is based on four main elements, namely: "any information", "concerning", "natural person", and "identified or identifiable". According to the [5], it is any information relating to a natural person who can be identified, directly or indirectly; for instance, a name, photo, fingerprint, postal address, email address, telephone number, social security number, internal identification number, IP address, computer login ID, voice recording, etc.

The processing of personal data, and handling of personal data, includes various actions such as collection, recording, organization, storage, modification, association with other data, transmission, etc. Analyses of the legal and regulatory texts as well as the charters for the use of computer systems have highlighted the six axes on which the protection of personal data is based on the following points [6]:

1. Information: the obligation to inform the user about the processing,
2. Consent: the consent expressed by the data owner to the collection and processing of his/her personal information,
3. Modification: includes several rights of the data owner, among others: access, update, and deletion of the data collected and processed,
4. Justification: Justify the purpose of the data processing by answering the question: "Is it justified to collect such data and use it in the context of such and such processing?"
5. Storage: the period of storage of personal data is limited in time and determined according to the context of the processing,
6. Transmission: The transmission of data to third parties must be limited and subject to authorization, in special cases, it is prohibited altogether.

In information systems, these axes are translated into guidelines, such as data protection by design, privacy impact assessment and data breach notification [7]. In [8] has defined the following eight strategies that IT architects should apply to embed privacy by design, as illustrated in Figure 1.

1. Minimize: Reduce the impact of a system on privacy as much as possible by collecting only the data strictly necessary for processing.
2. Hide: Hide personal data and its interrelationships to prevent abuse, for example, by using encryption.
3. Separate: Process personal data in a distributed manner, in separate compartments as soon as possible (K-anonymity, I-diversity).
4. Aggregate: Processing personal data at the most aggregated level possible, limiting the details.
5. Inform: Ensure transparency by adequately informing data owners about the processing of their information.
6. Control: Give data subjects full right and control over their personal data.
7. Impose: Implement a privacy policy that complies with legal requirements and ensure it's applied.
8. Demonstrate: Enable the Data Controller to prove compliance with the Privacy Policy and applicable legal requirements.

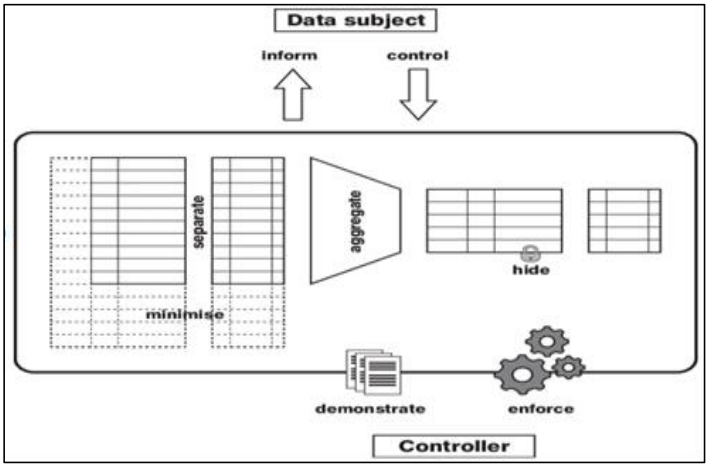

Figure 1: Strategies for personal data privacy.
Source: Authors, (2025).

II.2 THE NATIONAL AUTHORITY FOR THE PROTECTION OF PERSONAL DATA

The National Authority for the Protection of Personal Data translated in French as 'Autorité Nationale de Protection des Données à carcartère Personnel' (ANPDP) is an independent administrative institution functionally attached to the Presidency of the Republic, created by Law 18-07 of 10 June 2018 [7] to protect natural persons in the processing of personal data. The headquarters of the ANPDP are located in Algiers (commune of Hydra) [8]. The ANPDP (Figure 2) is responsible for ensuring that the processing of personal data is carried out in accordance with the provisions of this law and for ensuring that the use of information and communication technologies does not involve threats to the rights of individuals, public freedoms, and privacy [9].

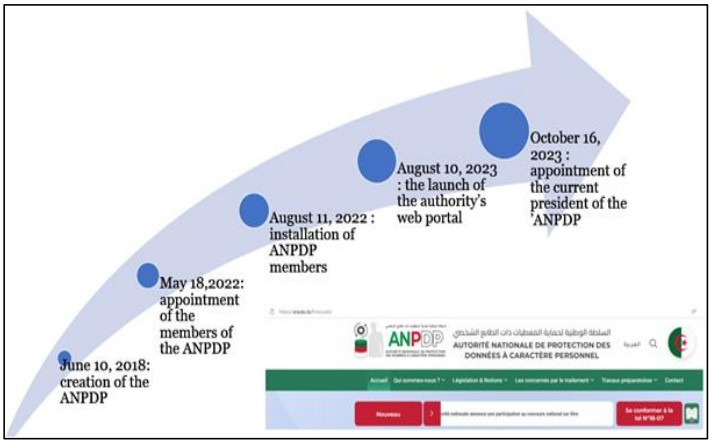

Figure 2: Timeline of the ANPDP.
Source: Authors, (2025)

The ANPDP's missions [9]:

1. To issue authorizations and receive declarations relating to the processing of personal data;
2. To inform data subjects and data controllers of their rights and obligations;
3. To advise persons and entities who use the processing of personal data or who carry out tests or experiments likely to lead to such processing;
4. To receive complaints, appeals, and complaints relating to the implementation of the processing of personal data and to inform their authors of the action taken on them;

5. To authorize, under the conditions provided for in this law, cross-border transfers of personal data;
6. To order the necessary changes to the protection of the personal data processed;
7. To order the closure of data, its removal or destruction;
8. To present any suggestions likely to simplify and improve the legislative and regulatory framework relating to the processing of personal data;
9. To publish the authorizations granted and the opinions issued in the national register referred to in Article 28 of Law 18-07;
10. To develop relations of cooperation with similar foreign authorities, subject to reciprocity;
11. To impose administrative sanctions under the conditions defined by Article 46 of this Law 18-07;
12. To develop standards in the field of personal data protection;
13. To draw up rules of good conduct and ethics applicable to processing personal data.

Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data is an important step forward in terms of the protection of individual freedoms, but also in the accountability of companies for the data they collect and the preservation of the privacy of natural persons who interact in both the production and consumption processes [10], [11]. It is structured in seven headings, as illustrated in the following Table 1.

Table 1: Structure of Law 18-07.

Titles	Chapters	Articles
General Provisions		1 - 6
Fundamental principles of personal data protection	Prior approval and data quality	7 - 11
	Pre-treatment procedures	12 - 21
The National Authority for the Protection of Personal Data		22 - 31
Rights of the data subject	Right to be informed	32 - 33
	Right of access	34
	Right to rectification	35
	Right to object	36
	Prohibition of Direct Marketing	37
Obligations of the Data Controller	Confidentiality and security of processing	38 - 41
	The processing of personal data related to certification and electronic signature	42
	Processing of personal data in the context of electronic communication	43
	Transfer of data to a foreign country	44 - 45
Administrative and penal provisions	Administrative procedures	46 - 48
	Rules of procedure	49 - 53
	Criminal provisions	54 - 74
Transitional and final provisions		75 - 76

Source: Authors, (2025).

II.3 THE UP PROCESS

For a better control of our project, the UP process has been integrated, which describes a two-pronged approach [12-14] (Figure 3).

A) A horizontal axis divided into four phases:
1. Inception: corresponds to the initialization of the project where a feasibility study of the system to be built is carried out.
2. Development: corresponds to the validation of the use cases resulting from the previous phase, the risk assessment and the study of the profitability of the project as well as the planning of the construction phase.
3. Construction: corresponds to the production of a first version of the product; it is focused on the phases of design, implementation and testing activities.
4. Transition: corresponds to the delivery of the product for a real operation where “beta tests “are carried out to validate the new system with users.
5. Iterations: an iteration is a complete development circuit that results in the delivery of an executable product.

B) A vertical axis that present the sequence of activities in the UP process:
1. Expression of needs: UP distinguishes between two types of needs. The functional needs that lead to the development of use cases, and Non-functional needs that result in the drafting of a requirements matrix.
2. Analysis: the analysis takes the form of the elaboration of all the diagrams giving a representation of the system, both static (mainly class diagram) and dynamic (diagram of use cases, sequences, activities, state-transitions, etc.).
3. Design: the design takes into account the technical architecture choices made for the development and operation of the system. The design extends the representation of the diagrams at the analysis level by integrating the technical aspects that are closest to the physical concerns.
4. Implementation: This phase corresponds to the production of the software in the form of components, libraries, or files.
5. Test: Tests verify the proper implementation of all requirements (functional and technical), the correct functioning of interactions between objects and the proper integration of all components into the software.

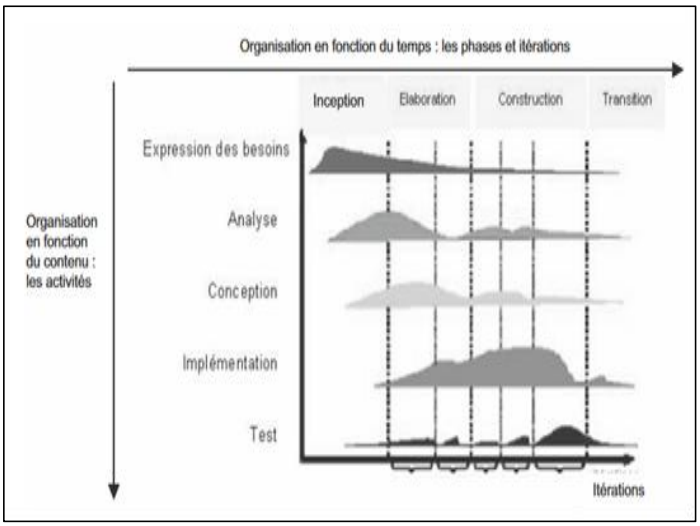

Figure 3: Overall diagram of the UP process.
Source: Authors, (2025).

III. MATERIALS AND METHODS

The main objectives of the preliminary study are to establish and initial collection of functional and operational requirements and to model the system context. Functional needs represent the main functionalities of the system [15],[16]. Non-functional requirements are indicators of the quality of the execution of functional requirements [17].

In this work, Microsoft Visual FoxPro V.9 (VFP) was used as the development environment for our application. The latter is a relational database management system (RDBMS) and an object-oriented programming environment designed to create database applications. Among the features of VFP, we can mention [18]:

- Rapid Application Development (RAD)
- Interactive Development Environment (IDE)
- Table and Database Management
- Data Connectivity

The functional needs are represented in Table 2.

Table 2: System functional requirements.

Needs	Features
Management of the register of personal data processing	The Data Controller (DC) monitors the application's processing. The Authorized Representative (AR) verifies the validity of the processing with Law 18-07 and ensures the follow-up of the declaration submitted to the ANPDP.
Management of the register of data subjects' rights	The Authorized Representative (AR follows the data subject's entitlement request and notifies third parties of the results. The DC processes the request for this right.
Management of the register of personal data breaches	The AR tracks the personal data breach in the app, develops the action plan preventive measures, notifies third parties, and closes the case. The Chief Information Security Officer (CISO) handles the breach.
Database Administration	The administrator : - Controls access to all features, - Manage the Database, - Saves and restores the Database, - Creates and modifies user profiles.
Authentication and access	The user must enter a password to access the app.

Source: Authors, (2025).

In our case, the non-functional requirements are translated into three points:

1. Security: The system administrator is responsible for defining the user profiler and storing passwords securely.
2. Educational: To provide an informative bridge between the operations of the system, on the one hand, and the legal essence of Law 18-07, on the other hand.
3. Usability: Integrate tooltips into the app to help users navigate and interact effectively with the app.

The dynamic context diagram of our application “Conform1807" is illustrated in Figure 4, we emerge with the identified actors of the system:

1. Main actors:
- The DC,
- The AR,
- The CISO,
- The administrator.
2. Secondary actor :
- The Data Subject (DS),
- The ANPDP

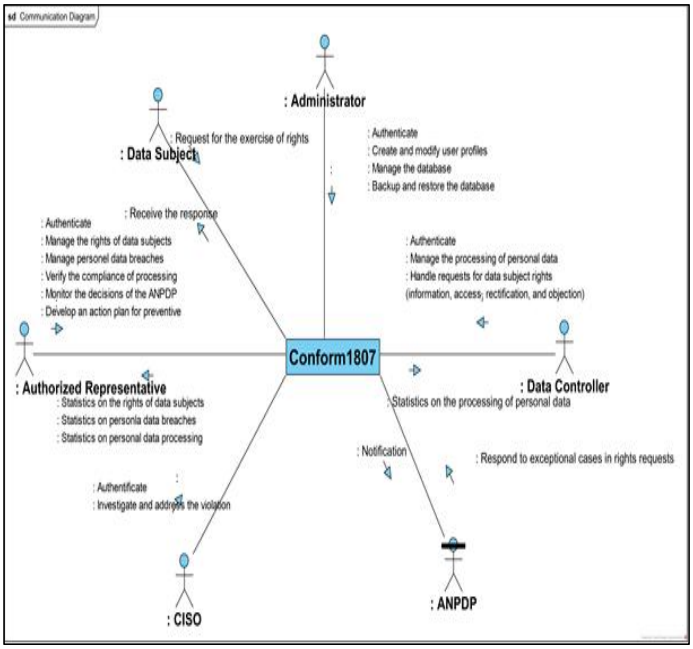

Figure 4: Dynamic context diagram of "Conform1807".
Source: Authors, (2025).

Table 3: Distribution of use cases and actors package.

Use cases	Actors	Package
Tracking the processing of personal data	DC	Management of the processing of personal data
Verify the compliance of personal data processing	AR	
Follow the decisions of the ANPDP	AR	
	ANPDP	
Follow up on the right request of the data subjects	AR	Management of data subject rights requests
	DS	
To process the data subjects' request for rights	DC	
	ANPDP	
Track the personal data breach	AR	Management of personal data breaches
	ANPDP	
	DS	
Handling the breach of personal data	CISO	
Manage users	Administrator	Support service
Manage the Database		

Source: Authors, (2025).

The Use Case Diagram (UCD) identifies four main and two secondary actors (Figure 5):

- Main actors: the data controller, the AR, the CISO and the administrator.
- Secondary actors: the ANPDP and the data subject.

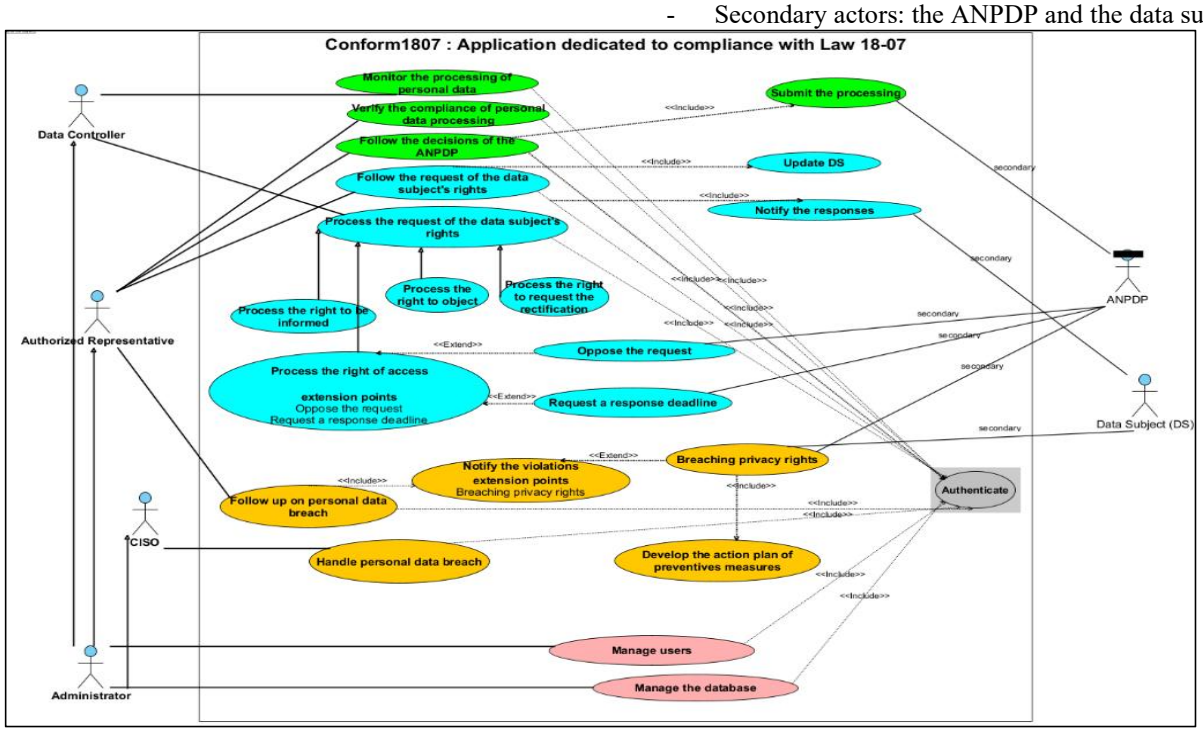

Figure 5: Use case diagram.
Source: Authors, (2025).

In the activity diagram of the “management of personal data processing”, there are two main actors and one secondary actor, as illustrated in Figure 6.

1. The data controller, the main actor, monitors the processing of personal data.
2. The Authorized Representative, the main actor, verifies the compliance of the processing with respect to Low 18-07 and prints the processing declaration to be submitted to the ANPDP through the Web portal.
3. The ANPDP, a secondary actor, receives the treatment declaration.

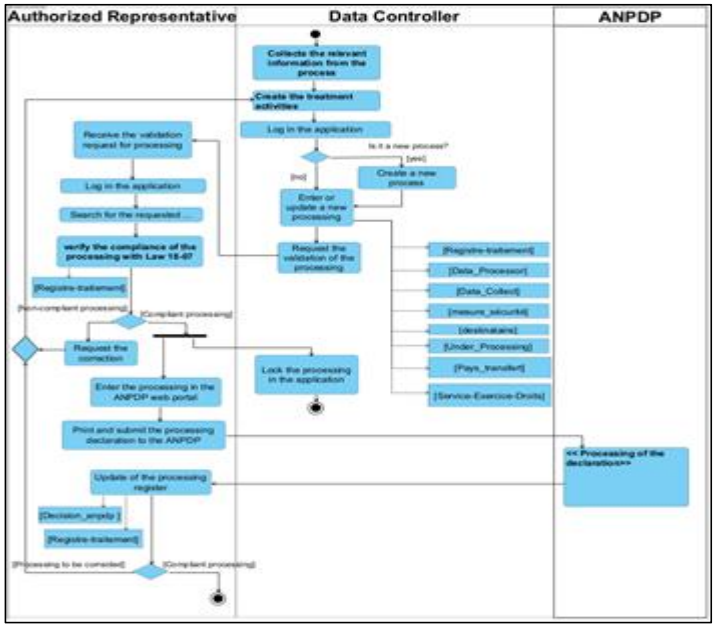

Figure 6: Activity diagram of the Management of Personal Data Processing package.
Source: Authors, (2025).

In the activity diagram of the "Management of Data Subjects' Rights Requests", there are two main actors and two secondary actors, as illustrated in Figure 7.

1. The AR, receives the request for rights from the concerned person and follows up on the rights request. He documents the results and notifies third parties.
2. The data controller, as the main actor, processes the request for the rights of the data subjects.
3. The data subject, who is a secondary actor, requests the exercise of these rights.
4. The ANPDP, a secondary actor, responds to requests for response time.

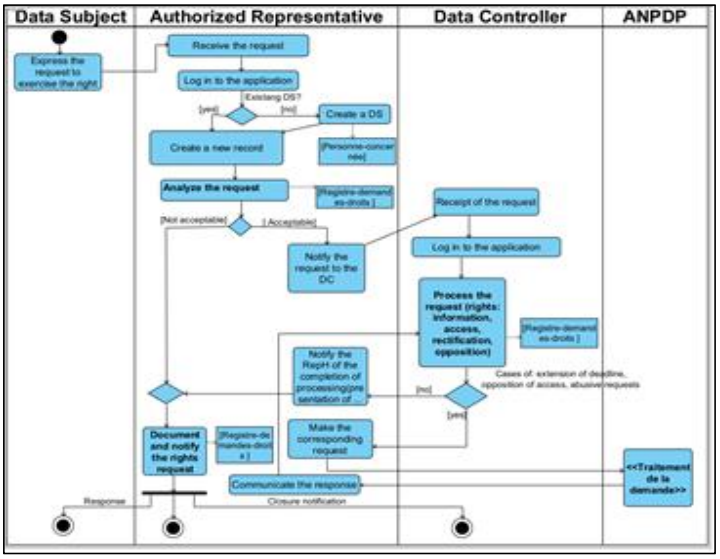

Figure 7: Activity diagram of the Management of Data Subjects Rights Requests package.
Source: Authors, (2025).

In the activity diagram of the Personal Data Breach Management, there are two main actors and one secondary actor, as illustrated in Figure 8.

4. The AR, he main actor, monitors the violation of personal data. He notifies third parties of the breach.

5. The CISO, the main actor, send the report of detection of the personal data breach to the AR, addresses the breach, and develops the action plan for preventive measures.

6. The ANPDP and the concerned person, secondary actors, receive notifications of violations.

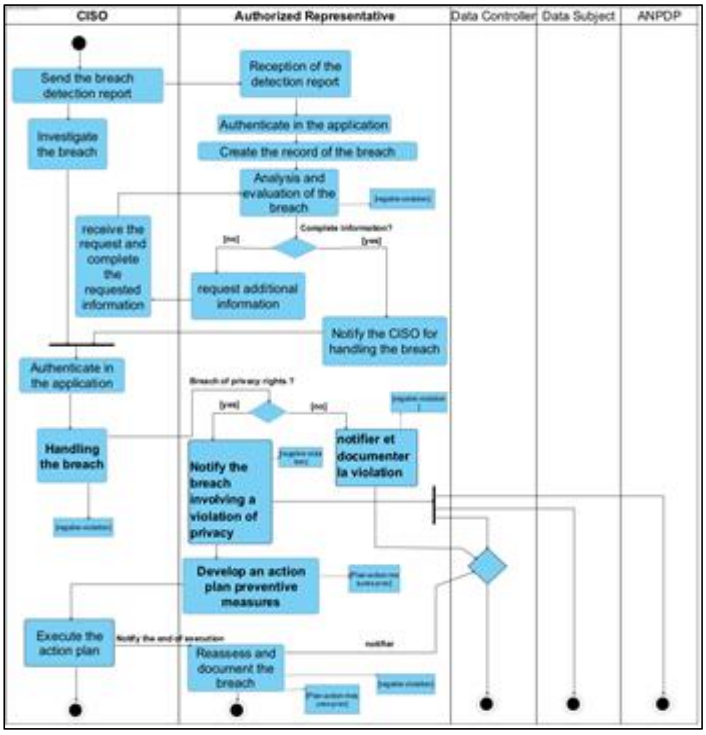

Figure 8: Activity diagram of the “Personal Data Breach Management" package.
Source: Authors, (2025).

The class diagram of our application is shown in Figure 9.

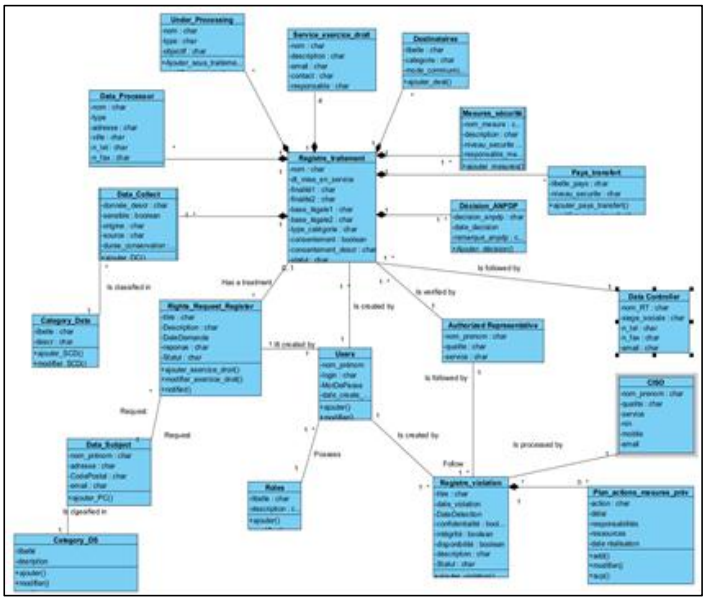

Figure 9: Class diagram.
Source: Authors, (2025).

In our application, we implemented the SHA-256 hashing algorithm to secure user passwords, as shown in Figure 10.

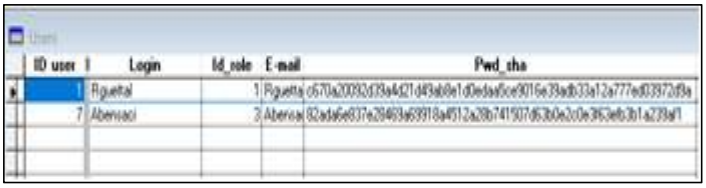

Figure 10: User table with hashed password field (Pwd_sha).
Source: Authors, (2025).

IV. RESULTS AND DISCUSSIONS

To access the application named Conform1807, the user must authenticate with username and password (Figure 11).

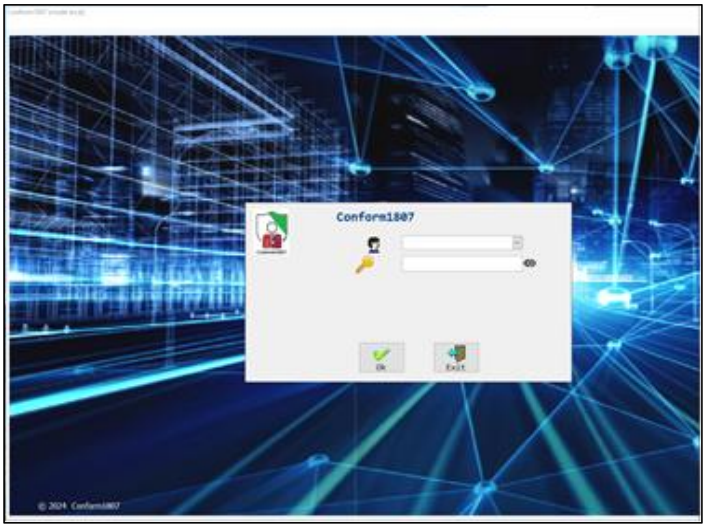

Figure 11 : The “Authentication” interface.
Source: Authors, (2025).

The Roles interface (Figure 12) , allows configuring system access permissions, thus ensuring system protection.

Figure 12 : The “Roles” interface.
Source: Authors, (2025).

In order to manage users, the “User Management” interface is implemented, as shown in Figure 13.

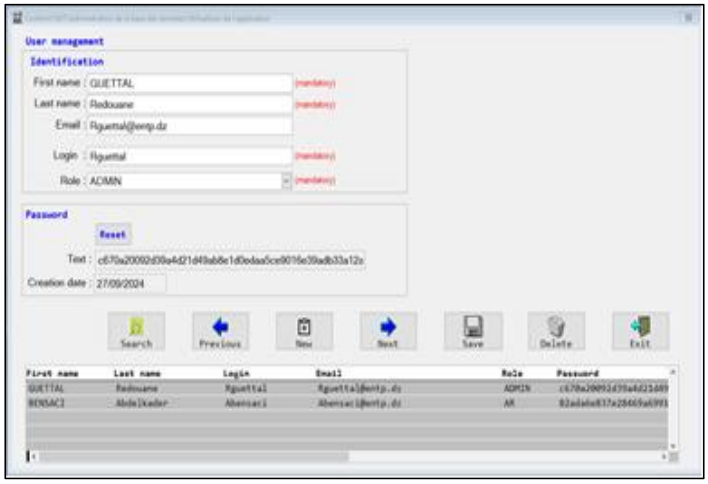

Figure 13 : The “User Management” interface.
Source: Authors, (2025).

In the Conform1807 application, the management of the personal data processing register is carried out through the interface shown in Figure 14.

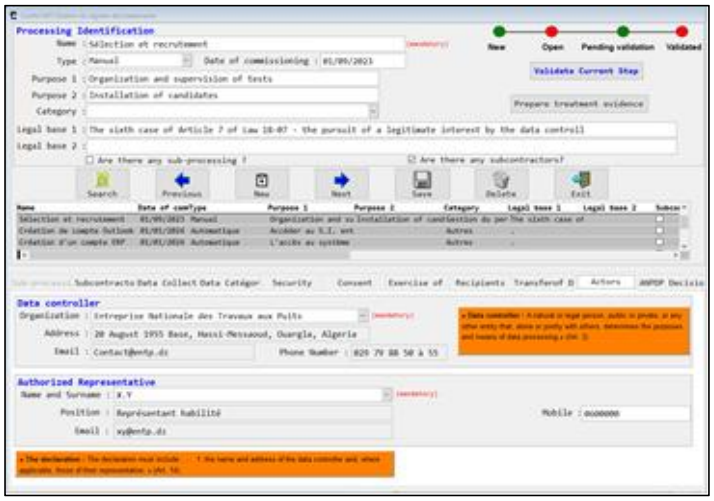

Figure 14 : The interface of the “Personal data processing management” module.
Source: Authors, (2025).

Managing data subject rights requests begins with identifying the concerned person, as illustrated in Figure 15.

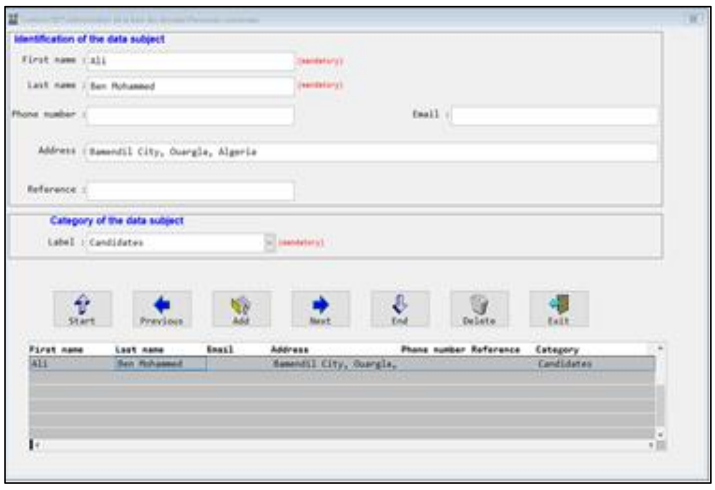

Figure 15: “Data Subjects Update” interface.
Source: Authors, (2025).

Once the data subject is identified, the request is tracked and recorded in the associated registry, as illustrated in Figure 16.

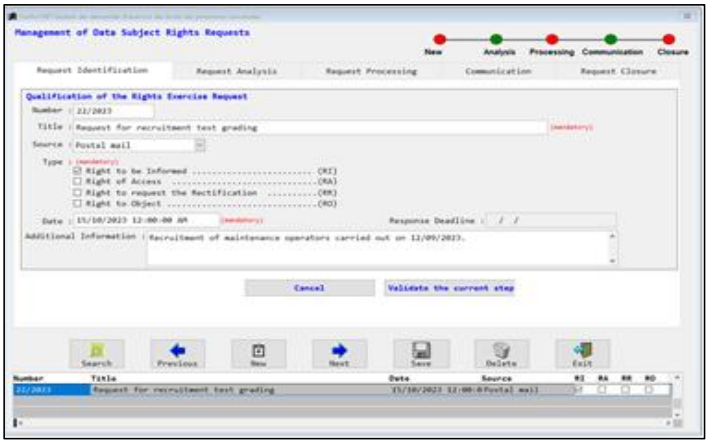

Figure 16 : The interface of the "Management of requests for rights of data subjects".
Source: Authors, (2025).

The CISO and AR handle the personal data breach register, as explained in Figure 17.

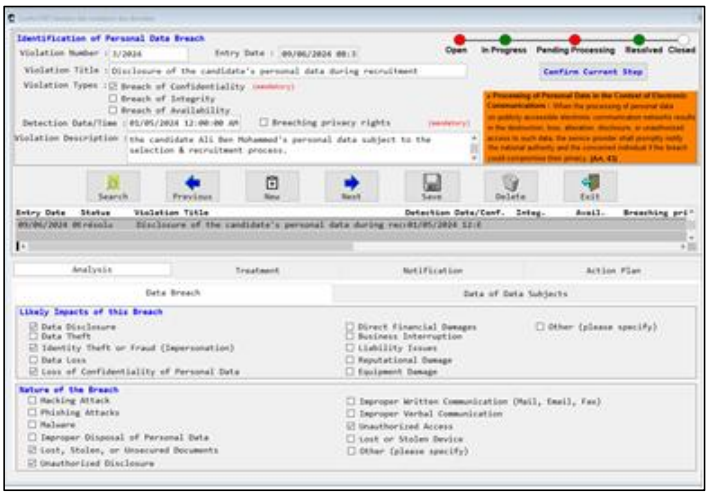

Figure 17: The interface of the “Personal Data Breach Management” module.
Source: Authors, (2025).

Our application "Conform1807" stands out for its ability to provide companies with an effective tool to comply with the requirements of Law 18-07; it incorporates the principles of personal data protection such as individuals' rights, notification of personal data breaches as an example, and not exhaustively. By offering a user-friendly interface, automated compliance assessments, and personalized advice, it meets a critical need in the local market.

V. CONCLUSIONS

Law 18-07 marks a significant step forward in Algeria's legal framework for personal data protection, aiming to regulate data processing comprehensively while ensuring the rights of individuals. However, compliance presents technical and organizational challenges, with risks of legal sanctions and reputational harm.

Addressing these issues, our application offers a local, accessible solution tailored to Algerian companies, filling a

critical gap by providing a user-friendly tool that facilitates data processing management, respects individuals' rights, and handles data breaches effectively, all while considering the specificities of algerian legislation and avoiding the high costs and complexity of international alternatives.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Redouane Guettal, Mohammed Kamel Benkaddour.
Methodology: Redouane Guettal, Mohammed Kamel Benkaddour.
Investigation: Redouane Guettal, Mohammed Kamel Benkaddour.
Discussion of results: Redouane Guettal, Mohammed Kamel Benkaddour.
Writing – Original Draft: Redouane Guettal.
Writing – Review and Editing: Mohammed Kamel Benkaddour.
Resources: Redouane Guettal, Mohammed Kamel Benkaddour.
Supervision: Mohammed Kamel Benkaddour.
Approval of the final text: Redouane Guettal, Mohammed Kamel Benkaddour.

VII. REFERENCES

[1] A. Elguerri, "Protection Of Audiovisual Personal Data in the Digital Environment: Analytical study of Algerian law No. 18-07 on the Protection of Natural Persons with regard to the processing of personal data," Arab International Journal for Information Technology & Data, vol. 3, no. 1, pp. 117–132, 2023.

[2] Z. Sipos, "CYBERSECURITY IN ALGERIA," Journal of Security & Sustainability Issues, vol. 13, no. 1, 2023.

[3] A. F. Westin, Privacy and Freedom. Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure, and Surveillance. Columbia Law Review 66, 1205–1253 ,1966.

[4] I. Coulibaly. The protection of personal data in scientific research. Ph.D dissertation, Grenoble Univ., Grenoble, France, 2011.

[5] CNIL, "Commission Nationale de l'Informatique et des Liberté.,https://www.cnil.fr.

[6] C. De Terwangne, "Council of Europe convention 108+: A modernised international treaty for the protection of personal data," Computer Law & Security Review, vol. 40, p. 105497, 2021.

[7] W. B. Chik, "Generative Artificial Intelligence: The Protection of Personal Data and Countering False Narratives about the Person," SAcLJ, vol. 36, p. 307, 2024.

[8] J. H. Hoepman, "Privacy Design Strategies", 2013, *arXiv:1210.6621v2.*

[9] Law No. 18-07, June 10, 2018, Official Journal of the Algerian Republic (JORA), no. 34, June 10, 2018.

[10] ANPDP, "The National Authority for the Protection of Personal Data," 2024.

[11] Z. YACOUB, "On the protection of personal data in light of law n° 18-07: a new responsibility for companies", Academic Review of Legal Research (RARJ), Jun. 2021.

[12] Y. Kovalenko, "The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights," Masaryk University Journal of Law and Technology, vol. 16, no. 1, pp. 37–57, 2022.

[13] E. Gefenas, J. Lekstutiene, V. Lukaseviciene, M. Hartlev, M. Mourby, and K. Ó. Cathaoir, "Controversies between regulations of research ethics and protection of personal data: informed consent at a cross-road," Medicine, Health Care and Philosophy, pp. 1–8, 2022.

[14] E. Gefenas, J. Lekstutiene, V. Lukaseviciene, M. Hartlev, M. Mourby, and K. Ó. Cathaoir, "Controversies between regulations of research ethics and protection of personal data: informed consent at a cross-road," Medicine, Health Care and Philosophy, pp. 1–8, 2022.

[15] S. C. Salim and J. Neltje, "Analysis of Legal Protection Towards Personal Data in E-Commerce," in 3rd Tarumanagara International Conference on the Applications of Social Sciences and Humanities (TICASH 2021), Apr. 2022.

[16] N. S. Haliwela, "The Essence of Legal Protection of Personal Data of Customers In Banking Transactions," SASI, vol. 29, no. 3, pp. 548–556, 2023.

[17] M. Durovic and T. Corno, "The privacy of emotions: From the GDPR to the AI Act, an overview of emotional AI regulation and the protection of privacy and personal data," Privacy, Data Protection and Data-driven Technologies, pp. 368–404, 2024.

[18] Inter Soft Associates, "Visual FoxPro's Advanced Technical Features Included Complex Data Processing," 2024.