WHISTLEBLOWING PLATFORM

OpenBlow® is the leading platform for reporting illegal conduct, designed for **Public Administrations** and **Private Organizations**. It natively complies with directives and regulations related to Whistleblowing and Privacy.

It was developed in collaboration with the National Anti-Corruption Authority (**ANAC**), and thanks to this partnership, the platform ensures full compliance with all **legal requirements concerning whistleblowing**.

The Regulation

Law 179/2017 and **Legislative Decree 231/2001**, which began defining the whistleblowing framework in Italy, already provided for the adoption of an IT tool within **Public** and **Private Organizations**. This tool allows employees to report potential fraud, a crime, an offense, or any irregular conduct committed by other members of the organization to specific individuals or bodies (including law enforcement and public authorities).

On **March 30, 2023, Legislative Decree 24/2023 came into effect to implement Directive (EU) 2019/1937**, concerning "the protection of persons who report breaches of Union law and containing provisions regarding the protection of persons who report breaches of national regulatory provisions." The decree expanded the scope of application and imposed the obligation to provide reporting channels that ensure the protection of the individuals involved and mentioned in the report, and allow for timely and efficient management.

The subjects obligated under whistleblowing regulations according to the law are identified in Articles 2 and 3 of Legislative Decree 24/2023:

- **Public Sector Entities:** Public administrations, Independent administrative authorities, Economic public entities, Public service concessionaires, Publicly controlled companies, In-house companies, even if listed.
- **Private Sector Entities that:**
  1. Have employed, in the last year, an **average of at least 50 employees** with permanent or fixed-term contracts;
  2. Fall within the scope of Union acts referred to in Parts I.B and II of the annex to the decree, **even if in the last year they did not reach an average of 50 employees**; these include sectors such as financial services, products, and markets, prevention of money laundering and terrorist financing, as well as transport security;
  3. Are different from the entities mentioned in the previous point, have an **organizational and management model 231**, even if in the last year they did not reach an average of 50 employees.

INFO@LASERROMAE.IT

STRENGTHS

The **OpenBlow platform is a web-based application** and is accessible from any PC and mobile device.

- **Web-Based** IT Platform.
- **Simplification** of report management procedures.
- **Confidential** and **encrypted** report **content**.
- **Separation of the whistleblower's identity** from the report.
- Appropriate data **access** and **retention policies**.
- **Integration** of the platform into existing environments.
- **Available** in any language.

Whistleblower Protection

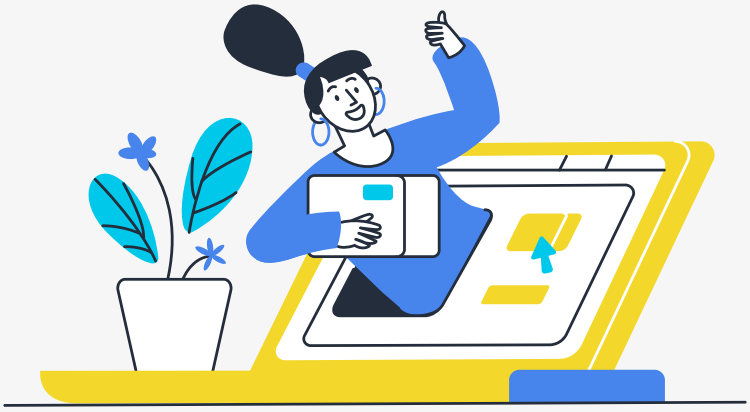
Legislative Decree 24/2023 provides Whistleblowers with a protection system to **safeguard their identity**, protect them from retaliation, and **ensure immunity** from penalties related to industrial secrecy (Article 54-bis of Legislative Decree No. 165/2001).

- **Protection of the Whistleblower's Identity**
  The identity of the whistleblower cannot be disclosed to anyone other than those competent to receive or follow up on the reports.

  Protection covers not only the name of the whistleblower but also any elements of the report that might indirectly reveal the whistleblower's identity;

- **Protection Against Retaliatory or Discriminatory Measures Following a Report**
  Any behavior, act, or omission, even if merely attempted or threatened, carried out as a result of the report, judicial or accounting complaint, or public disclosure, **that causes or may cause unjust harm to the whistleblower or the person who made the complaint, either directly or indirectly, is considered unjustified harm.**

- **Immunity for Whistleblowers**
  Whistleblowers are not subject to penalties for revealing or disseminating information about breaches covered by confidentiality obligations (excluding professional forensic and medical secrecy, copyright protection, or personal data protection), provided that, at the time of the report, complaint, or disclosure, they had reasonable grounds to believe that revealing or disseminating the information was necessary to make the report and that the report was made in accordance with legal requirements.



OBJECTIVE

The goal of Whistleblowing is to enable Organizations to address reported issues in a timely and effective manner, identifying situations of risk or harm and contributing to the prevention and combating of potential illegal activities.

- **Whistleblowing Actors**
  The main actors involved in the Whistleblowing process interact securely and confidentially through the OpenBlow® platform.
- **Handling of Reports**
  The management of reports regarding illegal conduct is organized into sequential phases, structured within a process implemented and fully automated through the platform.

Whistleblowing Process

The Whistleblowing process is centralized on the platform, which ensures a clear separation of roles and security throughout all phases of report management. Upon receiving a report, the designated person proceeds with the following steps:

- **Categorization** of the report;
- **Preliminary verification** of the report (screening);
- **Investigation** (and interaction with the Whistleblower);
- **Resolution** (closure) with outcomes of either archiving or forwarding;
- **Transmission to Competent Offices** and/or internal departments if forwarded.

01.

REPORT SUBMISSION

02.

PRELIMINARY VERIFICATION

03.

INVESTIGATION

04.

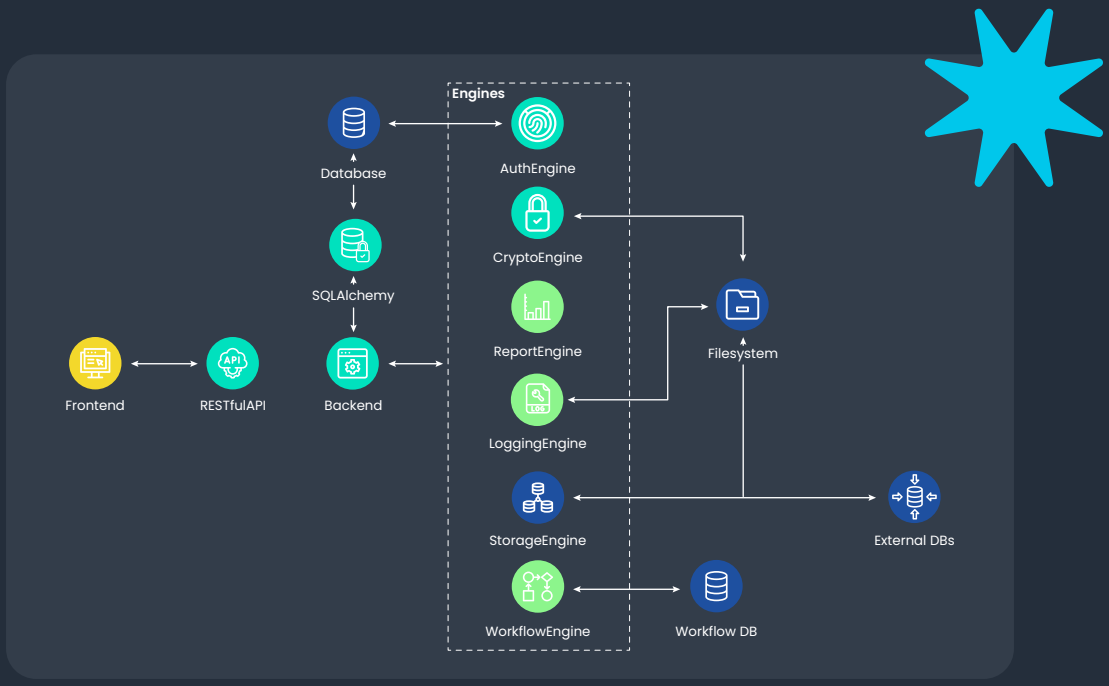
INTERACTIONS WITH OTHER ACTORS

The Platform

The Whistleblowing platform was designed and implemented by the Laser Romae development team, with the aim of creating a secure, easy-to-use product that is integrable into any type of Organization.

Platform Architecture

The platform features a multi-engine architecture to facilitate easy integration into heterogeneous environments. The modularity of the platform allows each core functionality to use plugins to connect to existing systems (e.g., BPMN, queue systems, storage systems).



Service Delivery Modes

The Whistleblowing service is provided both in **SaaS** (Software as a Service) mode and in **on-premise** mode on the Client's infrastructure.

Saas

The Whistleblowing service is provided in SaaS mode through Laser Romae's data centers located in Europe.

Service Features:

- Infrastructure provisioning
- Platform deployment
- Platform operation
- Staff training
- Support
- Corrective and adaptive maintenance
- Evolutionary maintenance
- Service decommissioning
- Data migration

On-premise

The Whistleblowing platform can be installed on-premise in the Client's data centers and integrated into the infrastructure.

Service Features:

- Platform installation
- Configuration/Tuning of the platform
- Platform operation
- Staff training
- Support
- Corrective and adaptive maintenance
- Evolutionary maintenance
- Data migration

THE PLATFORM

The platform, in addition to allowing the reporting of illegal activities using digital methods, natively complies with **ANAC directives** and relevant regulations:

- **Separate the whistleblower's identity from the content of the report** by adopting substitute codes for identifying data so that the report can be processed anonymously and allows for the subsequent reconstruction of the whistleblower's identity only in permitted cases;
- **Manage reports transparently** through a defined procedural process communicated externally with clear terms for initiating and concluding the investigation;
- Maintain **confidentiality of the report content** throughout the entire management phase of the report;
- Adopt **secure protocols for data transmission over the network** and use encryption tools for report contents and any attached documentation;
- Adopt **appropriate data and documentation retention methods** (physical, logical, hybrid);
- Implement **confidentiality protection policies** through IT tools (decoupling the whistleblower's identity from the report information, encryption of data and attached documents);
- Adopt **data access policies** (authorized officials, system administrators).

Security

Regarding Cybersecurity aspects, ANAC has requested the execution of an Application Security Assessment (ISO 27001, OWASP) of the platform in pre-operation and operational environments.

Key Security Features:

- **Data Retention Policy**
  Each report stored in the Database increases attractiveness for potential hackers.
  Reports have an expiration date that can be extended by the Receiver.
  Expired reports are removed along with all their data.
- **Server Resiliency**
  The server is configured to neutralize DDoS attacks. Massive requests from the same IP address that could be considered an attack are automatically blocked.
- **Password storage**
  Passwords are stored using a hash generated with a random 128-bit salt. Whistleblower receipts are encrypted using the Crypto module. Python's random is used to generate a 16-digit code.
- **Web content security**
  Communication between front end and back end uses international best practices, including security headers and TLS 1.3 encryption.
- **File encryption**
  Report attachments, along with the report itself, are encrypted using the selected Crypto Engine. Default encryption offered is AES 256.
- **GDPR**
  The Whistleblowing Platform complies with the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679).