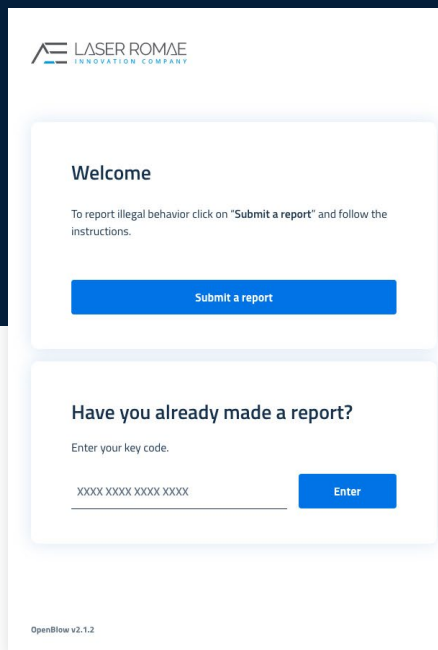


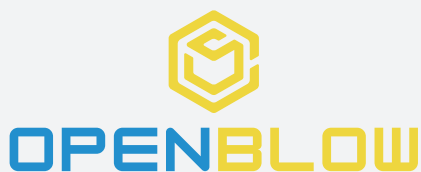
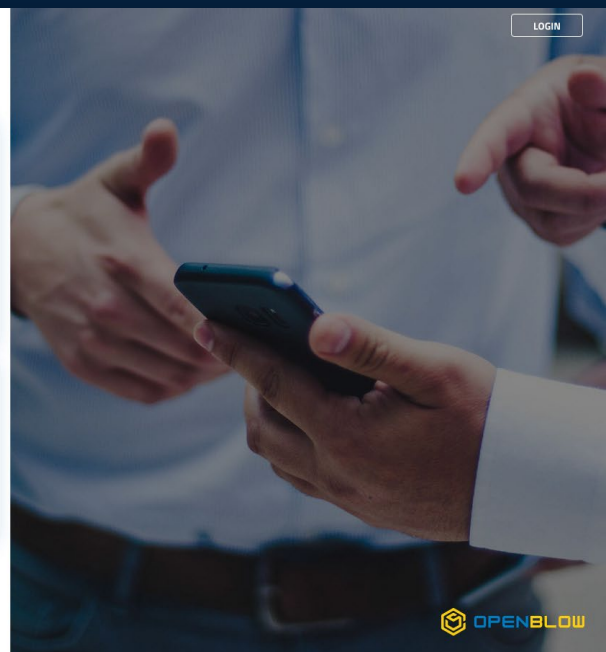
# Whistleblowing Open Source platform

**OpenBlow®** is the platform developed to report illegal conducts intended for **Public Administrations** and **Private Organizations**, which natively complies with the directives and reference standards on the subject of Whistleblowing and Privacy.

Born from the collaboration of **ANAC** and **Laser Romae**, which resulted in the Open Source availability of the platform developed by Laser Romae.



The screenshot shows the OpenBlow web interface. At the top left is the 'LASER ROMAE INNOVATION COMPANY' logo. Below it, a 'Welcome' section contains the text: 'To report illegal behavior click on "Submit a report" and follow the instructions.' A blue button labeled 'Submit a report' is centered below this text. Below the button is a section titled 'Have you already made a report?' with the instruction 'Enter your key code.' A text input field contains 'XXXX XXXX XXXX XXXX' and a blue 'Enter' button is to its right. At the bottom left of the interface, the text 'OpenBlow v2.1.2' is visible.



## Strength points

The Whistleblowing platform is a responsive Web-Based application and it is accessible from any PC and mobile device.

- IT platform **Web-Based**
- **Simplification** of reports management procedures
- **Confidentiality** of the reports content
- **Separation of the reports** metadata from its content
- Established **data access** and **retention policies**
- Platform **integration** in pre-existing environments
- Easy integration of **any language**

## The legislation

**Law 179/2017** and **Legislative Decree 231/2001** foresee for the adoption of an IT instrument within **Public** and **Private Organizations**, through the which employees report, to specific individuals or organization (including police and public authorities) a possible fraud, a crime, an offense or any irregular conduct committed by other persons belonging to the organization.

On **September 3rd 2020**, the **new regulation came into effect, allowing the National Anti-Corruption Authority to exercise the sanctioning power** in a more efficient and faster way.

**Four types of proceedings** have been established:

- handling reports of offenses;
- penalty procedure to verify the adoption of anti retaliatory measures;
- penalty procedure to verify the inertia of the Prevention of Corruption and Transparency Responsible (RPCT) in carrying out verification and analysis of the reports;
- penalty procedure to verify the absence of procedures for the forwarding and management of reports through IT platforms.

## Whistleblower protection

Law 179/2017 and Legislative Decree 231/2001 foresee the adoption of an IT instrument within the Public and Private Organizations, a system to **protect the confidentiality of the Whistleblowers identity**, in order to protect from possible retaliation and from any liability related to IPRs (art. 54 bis del d.lgs. n. 165/2001).

- **Protection of the confidentiality of the whistleblower identity**

Art. 54-bis requires the Public Administration to ensure the confidentiality of the whistleblower's identity.

- **Protection from any retaliatory or discriminatory measures following a reporting**

The law states that the employee who makes a report, cannot be sanctioned, demoted, fired or transferred and in no way penalized.

- **Exclusion from the responsibility to disclose information covered by the obligation to secret and / or fidelity**

The whistleblower is protected and is not held responsible if he/she complies with the methods provided for by law and uses the correct communication channels.

### Goal

Whistleblowing's goal is to allow organizations to address the reports in a timely and effective manner, drawing attention to risk or damage situations and contributing to the prevention and contrast of any offenses.

- **Whistleblowing actors**

The main actors involved in the Whistleblowing process interact with each other in a secure and confidential way through the OpenBlow® platform.

- **Processing of reports**

The unlawful conduct reports management is organized in sequential steps, structured within an implemented and fully automated process through the platform.

## Whistleblowing process

The Whistleblowing process is based on the platform, which guarantees a clear separation of roles and safety during all phases of reporting management. Upon receipt of a report, the designated person proceeds with the following steps:

- **Categorization** of the report;
- **Preliminary verification** of the report (screening of the report);
- **Preliminary investigation** (and interaction with the Reporting party);
- **Definition** (closure) ending with archiving or forwarding outcome;
- **Transmission to the competent offices** and/or internal departments in case of forwarding.



**01.**

**REPOR  
INTRODUCTION**



**02.**

**PRELIMINARY  
VERIFICATION**



**03.**

**PRELIMINARY  
INVESTIGATION**



**04.**

**FLOWS WITH  
OTHER ACTORS**

The platform, in addition to enabling the offenses reporting using digital means, complies natively to the **ANAC93 directives** and to the reference standards:

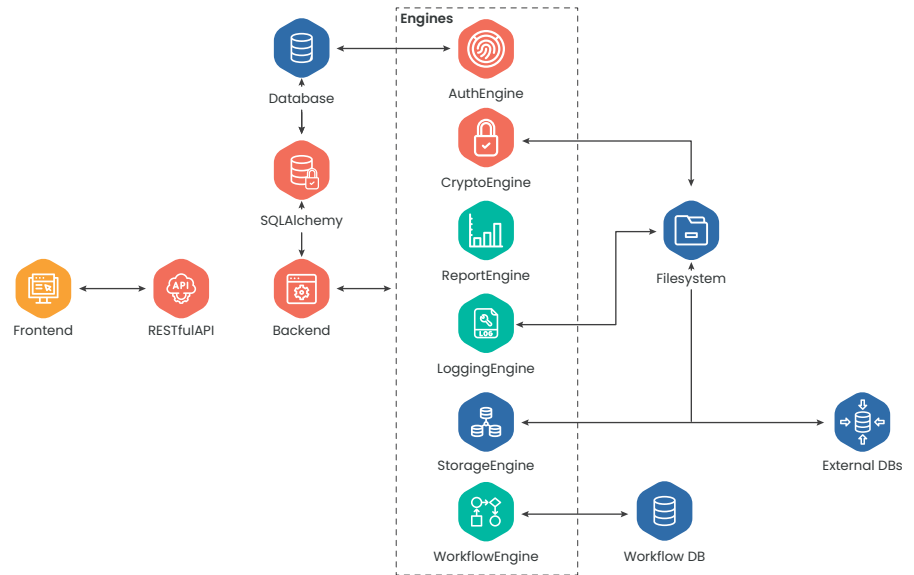
- **separate the identity data from the content of the report**, with the adoption of replacement codes in the identification section, so that the reports can be processed anonymously. Identity data can be linked to the report content only in permitted cases;
- **manage the reports in a transparent way**, through a well known, defined and public process with defined time frames for the start and the end of the preliminary investigation;
- **keep the content of the reports secure**, during the entire phase of reporting management;
- **adopt safe protocols** for the data transport over the network as well as the usage of cryptographic tools for the reports contents, identity and attachments;
- adopt adequate methods of **data retention** and documentation (physical, logical, hybrid);
- adopt policies to **protect the confidentiality** through IT tools (decoupling of identity data and reports, data encryption also for the attached documents);
- adopt **data access policies** (access to authorized users, system administrators).

## The platform

The Whistleblowing platform was designed and implemented by the Laser Romae development Team, with the goal of creating a safe product, easy to use and integrate in any type of organization.

### Platform architecture

The platform has a multi-engine architecture, for easy integration in heterogeneous environments. The modularity of the platform allows, for each of the core features, the deployment of plugins to connect to pre-existing systems (e.g. BPMN, queuing systems, storage systems).



### Delivery mode

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

#### • SaaS

The Whistleblowing service is provided in SaaS mode within Laser Romae's Datacenters located in Europe.

##### Service features:

- Infrastructure provisioning
- Platform Deployment
- Platform Operation
- Staff training
- Support
- Corrective and adaptive maintenance
- Perfective maintenance
- Service hand-over
- Data migration

#### • ON-PREMISE

The Whistleblowing platform can be installed on-premise in the Customer's datacenter and integrated within the infrastructure.

##### Service features:

- Platform installation
- Platform configuration / tuning
- Platform Operation
- Staff training
- Support
- Corrective and adaptive maintenance
- Perfective maintenance
- Data migration

## Cyber Security

Regarding the aspects related to Cyber Security, ANAC has requested the execution of an Application Security Assessment (ISO 27001, OWASP) in the preoperational and operational environments.

The main security features of the Platform are:

- **Data retention policy**

Each report stored in the database increases the attractiveness for potential hackers. Reports have an expiration date which can be extended by the Receiver, an expired report is removed with all its related data.

- **Server resiliency**

The Server is configured to prevent D/DOS attacks. Massive requests from the same IP address that can be traced to an attack are automatically inhibited.

- **Password storage**

Passwords are stored with a salted 128-bit randomly generated hash. Receipts for the whistleblowers are encrypted using the Python Crypto.Random module, and they are in the form of 16 digits code.

- **Web content security**

Communication between front and back end uses best practices, shared at international levels, including security headers and it is encrypted with TLS 1.3.

- **File encryption**

The report attachments, and the report itself, are encrypted using the selected Crypto Engine. The default one offers an AES 256 encryption.

- **GDPR**

La Piattaforma di Whistleblowing è a norma con il regolamento  
The Whistleblowing Platform complies with the general data protection regulation (GDPR - General Data Protection Regulation, EU regulation 2016/679).



[facebook.com/laserromae](https://facebook.com/laserromae)

[twitter.com/LaserRomae](https://twitter.com/LaserRomae)

[linkedin.com/company/laserromae](https://linkedin.com/company/laserromae)

[www.laserromae.it](http://www.laserromae.it)

Viale dell'Urbanistica, 15  
00144 Rome

+39 06 56559245

[info@laserromae.it](mailto:info@laserromae.it)

Copyright © 2021 Laser Romae