HOW TO SET-UP AN INITIATIVE TO PROVIDE ONLINE WHISTLEBLOWING PLATFORMS TO PUBLIC AND PRIVATE ENTITIES

GUIDANCE

Whistleblowing Solutions (WBS) is a non-profit social enterprise that supports the fight against corruption through the research, development and provision of specific digital technology and operational support to anti-corruption organisations. These organisations, in turn, support whistleblowers in reporting malpractice worldwide.

The goal of WBS is to support the development of the GlobaLeaks free software and to foster a large community of those who support whistleblowers.

Authors: Susanna Ferro and Giovanni Pellerano, Whistleblowing Solutions; Giorgio Fraschini, Transparency International Italy; Marie Terracol, Transparency International

Reviewers; Marusa Babnik and Dagmar Sober, Transparency International Slovenia

Funded by
the European Union

This publication was produced as part of the “Speak Up Europe” project, which was funded by the European Union’s Internal Security Fund – Police.

www.whistleblowingsolutions.it

TABLE OF CONTENTS

GLOSSARY

Lead organisation: An organisation managing and implementing an initiative to provide secure online whistleblowing platforms, based on the GlobaLeaks software, to other organisations.

User organisation: A public or private organisation which adopts a whistleblowing platform.

Administrator: The person running the GlobaLeaks platform in a user organisation. Administrators perform the maintenance and overall management of the platform, and provide technical assistance to organisation staff handling the whistleblower reports, but do not have access to the reports.

Whistleblower: The person who submits a report through the GlobaLeaks platform.

Recipient: The person in a user organisation who is enabled to read, verify and analyse whistleblowers' reports. Recipients may also communicate with whistleblowers via the platform to solicit additional information and evidence, by exchanging messages, even anonymously.

Software as a Service (Saas): The provision, to a user organisation, of software via the cloud.

Infrastructure as a Service (Iaas): The provision, to a user organisation, of hardware to run the provider's services.

INTRODUCTION

This guidance provides step-by-step support for setting up and running an initiative providing safe, confidential whistleblowing platforms to public and private organisations.

The guide is aimed at civil society organisations (CSOs), public authorities and other **non-profit organisations** interested in providing high-standard, cost-effective online whistleblowing platforms to public and private organisations, replicating the Italian initiative WhistleblowingIT (WBIT) developed by Whistleblowing Solutions Social Enterprise (WBS) and Transparency International Italy (TI Italy). It provides a step-by-step support on the major considerations when setting up and running an initiative similar to WhistleblowingIT, building on both organisations' experience of creating and running WhistleblowingIT and supporting a pilot replica, *Linija Spregovori*!, carried out in Slovenia by the Transparency International chapter, under the "Speak Up Europe" project financed by the European Commission.

WHY PROVIDE ONLINE WHISTLEBLOWING PLATFORMS?

Whistleblowers have a key role in protecting the public, companies and institutions from undetected corruption, mismanagement and other misconduct, and their damaging consequences. They enable early detection of wrongdoing, giving organisations the opportunity to take action before a situation causes harm to the public, triggers liability or leads to serious financial losses and reputational damage.

An increasing number of countries now acknowledge the important role of whistleblowers and have adopted laws to protect them, including by requiring organisations to implement internal whistleblowing systems – also known as "speak up" or internal reporting mechanisms. Experience has shown that to be effective as powerful risk management and prevention tools, internal whistleblowing systems need to achieve certain standards.[1]

Such systems should provide safe channels to receive reports, protect those reporting from retaliation, and guide an organisation's response. Best practice, often reflected in legislation, mandates the provision of multiple reporting channels that are safe and easily accessible to all relevant stakeholders, and that enable reporting in writing and orally. Whistleblowing channels should allow safe communication between the whistleblower and the recipient, including the transfer of supporting documents. At least one channel should enable communication with anonymous whistleblowers. An online reporting platform is a way to fulfil these requirements.

[1] To help public and private organisations implement truly effective internal whistleblowing systems, Transparency International has developed comprehensive best-practice principles. The principles draw on lessons learned from the implementation of whistleblower systems across the globe and on Transparency International's experience working with public institutions, companies and whistleblowers. They can be used by organisations in all sectors and countries to set up and operate internal whistleblowing systems which provide safe reporting channels, protect those reporting from retaliation, and ensure the organisation acts on these reports.

WHISTLEBLOWINGIT: A SAFE, USER-FRIENDLY AND COST-EFFECTIVE ONLINE WHISTLEBLOWING PLATFORM

WBIT was developed in Italy to respond to an urgent need created by the entry into force of a new whistleblowing law in 2017. The law mandated all public administrations to implement a whistleblowing procedure through secure online reporting systems which use encryption to protect data. As soon it was adopted, many private consultancies started to offer online reporting platforms to public administrations, but not all complied with best practice and some were very overpriced.

In response, Whistleblowing Solutions and TI Italy drew on their experience promoting safe and effective whistleblowing to establish an initiative to provide a free, high-standard, encrypted reporting platform for all public administrations in the country. The initiative promotes whistleblowing based on best practices learned through national and international experience.

By promoting best-practice whistleblowing standards, rather than following a "tick-box" approach, these guidelines aim to affect how whistleblowing is perceived at national level. At a time where national laws transposing the EU Directive on Whistleblower Protection are pushing whistleblowing onto the public agenda, it is particularly critical that organisations seize the opportunity to establish strong whistleblower reporting and protection mechanisms, and affect the direction whistleblowing could take in the coming decades.

WBIT offers software-based whistleblowing services to all public and private organisations. Along with supplying organisations with software compliant with the law, the initiative goes further to promote best whistleblowing practice by providing complementary services and documentation – for example, regarding internal whistleblowing policies and procedures on data protection.

WBIT aims to reach all public administrations by offering a high-standard whistleblowing platform for free. It also tries to address the needs of other organisations obliged to implement a whistleblowing system (medium-sized private companies, publicly owned companies) by offering standard, affordable options, as well as bespoke versions of the platform for private and public organisations that require specific settings and configurations.

WHAT DIFFERENTIATES WBIT FROM OTHER ONLINE WHISTLEBLOWING PLATFORMS?

An initiative driven by the public interest

One of the distinguishing points of WBIT is that it is not limited to providing IT software. It has a broader mission to promote safe and efficient whistleblowing systems. The online reporting platform is a core element, but it is just part of a whistleblowing system.

The initiative's strength in the whistleblowing field rests not in its role as a service provider, but as a leading expert on whistleblower protection. The software itself must fulfil key criteria of security and ease of use, but more is needed to make a whistleblowing channel effective or even compliant with the law. WBIT's depth of whistleblowing expertise distinguishes it from other IT service providers offering whistleblowing platforms, earning trust and confidence from organisations which often see whistleblower protection as an administrative burden.

The GlobaLeaks software

GlobaLeaks is a free, open-source whistleblowing software package developed to support civil society in implementing secure whistleblowing platforms and procedures. It is a mature technology resulting from 13 years of research and development, already used by more than 30,000 organisations worldwide. A growing community of whistleblowing experts, developers, activists, lawyers and users contributes to the software Users include companies and public agencies implementing whistleblowing procedures for compliance and to prevent corruption, as well as CSOs and media outlets carrying out investigative journalism and work to protect human rights.

The GlobaLeaks software is open source, and is therefore fully transparent,[2] and free, allowing organisations to save resources. It is continuously improved via new functionalities for security, efficiency and ease of use.

Originally developed to support a single organisation implementing its own internal or external whistleblowing channel, the software has been further developed to enable an organisation to offer the software as a service (SaaS), by providing online whistleblowing platforms to other organisations. This guidance refers to organisations that offer the GlobaLeaks SaaS as 'lead organisations', while those they supply the platform to are 'user organisations'.

GlobaLeaks is designed to be simultaneously secure and accessible, as well as fully compatible with the latest laws and regulations on whistleblowing and data protection, including the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law, the General Data Protection Regulation (GDPR) and UNI CEI EN ISO/IEC 27001:2017. GlobaLeaks is designed around different types of user, with specific roles and access to data tailored to the operations they need to perform, in line with data protection and confidentiality rules.

Users of a GlobaLeaks platform in its basic configuration – when implemented by an organisation for its individual use – are divided into three groups:

- Whistleblowers: the individuals reporting malpractices through the platform, which is designed to optimise their user experience
- Recipients: the individuals mandated to manage whistleblowers' reports
- Administrators: the individuals configuring and running the GlobaLeaks platform. Administrators perform the maintenance and overall management of the platform, and provide technical assistance to recipients, but do not have access to whistleblowers' reports.

In the context of SaaS system set-up, this basic configuration of GlobaLeaks is available for each user organisation. There is also an additional type of user only available to the lead organisation: a "super" administrator, able to configure the platforms of all user organisations.

GlobaLeaks offers many advantages for lead organisations, user organisations and whistleblowers. It is mobile phone-friendly and entirely configurable from a web administration interface.

Security[3]

- GlobaLeaks features strong security by design and by default.
- GlobaLeaks' developers are always looking to improve security, and regularly make free security updates available to users. The software is subject to continuous public peer-review and periodic independent security audits.
- The software provides full data encryption of whistleblower reports and recipient communication.
- It conforms to industry standards and best practices for application security (such as OWASP – Open Worldwide Application Security Project).
- It offers complete protection against automated submissions, preventing any spam.
- Advanced file viewers and software functionalities ensure most of the management of the handling of the whistleblowing case can take place on the platform, limiting exposure of data and overall risks.

[2] Being open-source also amplifies the possibilities of continuous peer review and including the civil society in the continuous improvement of a digital public good, and users are in full control of the technology and can determine its evolution;

[3] You can find further information about GlobaLeaks security features on GlobaLeaks website.

Option of anonymous whistleblowing

- Whistleblowers can file a report without providing their names or contact information. A unique 16-digit code allows them to log back into the platform anonymously. This allows them to decide whether and when they want to divulge their identity to those handling their report.
- The recipient of the report and the (anonymous) whistleblower can communicate through the platform, even if the whistleblower remains anonymous.

Multiple languages:

- GlobaLeaks is available in more than 90 languages, including support for languages written right to left, such as Arabic.
- It allows an organisation to provide a platform in several languages, both for recipients and whistleblowers – an essential feature in organisations working in an international environment or in a country where several languages are used.

Rich customisation possibilities:

- Users can customise the look and feel of their platform, through use of their logo and chosen colour, styles, font and text.
- They can create multiple reporting channels – for example, by topic or department.
- They can also create and manage multiple whistleblowing sites – for example, for subsidiaries or third-party clients.
- An advanced design capability allows users to design their own questionnaires for whistleblower reporting.

User-friendly interface for handling reports.

An intuitive interface for receiving and analysing reports allows the recipient to:

- Use labels to categorise reports received, and search reports to locate one quickly.
- Assign case-management status, such as open or closed, to reports.
- Exchange files with the whistleblower, including multimedia files.
- Chat with the whistleblower, even if anonymous, to discuss the report, ask for additional information, and provide feedback and updates.

Questionnaire design capabilities

Having a well-designed questionnaire allows user organisations to collect structured and detailed information from whistleblowers, supporting more efficient and timely handling of the reports received. Useful features include:

- Grouping questions in sections or steps featuring a title and a description. This is visually easier for whistleblowers and provides structure, and is particularly important to make the reporting platform mobile-friendly.
- Offering hover boxes, in the form of a question mark near a word or sentence with rollover text, to clarify questions by providing additional information, such as definitions or examples.
- Configuring questions to so that they activate other questions or question groups, based on the whistleblower's previous responses.

See the GlobaLeaks website for further information about the software, such as security and technical features.

COMPLIANCE WITH NATIONAL LEGISLATION

The online whistleblowing platform provided to user organisations must be compliant with national legislation. The main laws and regulations that apply are generally those relating to whistleblower protection and privacy.

In addition to whistleblowing regulations, other legal requirements, which are not covered by this document, might apply. It is essential for the initiative's lead organisations to scope applicable national rules to ensure their service is fully compliant.

Formal and informal interactions and collaboration with relevant national authorities, such as those responsible for whistleblowing and data protection, are important to enable delivery of a state-of-the-art initiative.

WHISTLEBLOWING LEGISLATION

An increasing number of countries are user national whistleblowing legislation, often requiring organisations of a certain size or within particular sectors to establish internal whistleblowing channels and procedures which meet certain standards. For example, the EU Directive 2019/1937 on whistleblower protection introduced minimum standards for whistleblowing systems in EU countries.

Several legal requirements are common to many national whistleblower protection laws, and relevant for online whistleblowing systems. These include:

- Channels for receiving the reports must be designed, established and operated in a secure manner that protects the identity of the reporting person and any third party mentioned in the report, and prevents access to that information by non-authorised staff members.
- Channels should allow the transfer of supporting documents.
- Channels should enable the durable storage of information, in accordance with whistleblowing and data protection laws, to enable further investigation.
- Organisations should acknowledge receipt of a whistleblowing report within a strict, short timeframe – for example, seven days, under the EU Directive.
- Channels should enable communication between the whistleblower and the person handling their report throughout the follow-up process, to allow:

- The persons handling reports to provide regular feedback to whistleblowers on the follow-up of their reports
- Whistleblowers to clarify their report and provide additional information or evidence, and to share their concerns about risks of retaliation and the protection of their identity.

The GlobaLeaks software provides security and protection on a technological level. It protects the identity of the whistleblower, the person suspected of wrongdoing, and any other persons mentioned in a whistleblowing report submitted through the platform, and prevents access to the report by non-authorised personnel. However, adopting a GlobaLeaks platform does not guarantee that the channel will be operated in a secure manner, nor that the reports received will be handled securely.

This is why a whistleblowing initiative needs to offer more than a software solution. It needs to provide user organisations with recommendations, resources and guidance to adopt and implement whistleblowing procedures that comply with the law and best practice (see the section below, "Supporting effective whistleblowing systems").

A key advantage of an online reporting platform is that it requires whistleblowers to structure their report by answering a set of questions. It is essential that the default questionnaires provided to user organisations are designed by a whistleblowing expert to comply with national legislation and regulations on whistleblower protection, and reflect international standards and best practices.[4] These questionnaires need to be reviewed regularly and potentially amended to comply with changes in relevant regulations.

DATA PROTECTION

Whistleblowing is closely connected to the treatment of personal data. Compliance with rules such as the EU General Data Protection Regulation (GDPR) is essential. National privacy authorities are often strict over the protection of private data, and are keen to sanction possible violations. For online whistleblowing platforms, sanctions can be issued both against organisations using the platform and the organisation providing it, especially as the data is kept on the lead organisations' servers.

There are different levels of compliance concerning the protection of data.

Technological protection of data

GlobaLeaks is delivered, by design and by default, to protect all the data included in a report submitted by a whistleblower on the platform, including information on their identity and that of any person mentioned in the report. GlobaLeaks does not track the whistleblower's original IP address.

Appointment of data processors

- **Appointment of initiative partners and providers as external data processor**: The user organisation is the controller of personal data. The lead organisation manages the platform where the data is hosted, therefore it needs to be appointed by the user organisation as external data processor. The IT provider and the data server provider, where there is one, must be appointed as data sub-processors. To ensure compliance, consistency and expediency, the lead organisation should develop a standardised data processor appointment form, and provide this to user organisations for signature, bearing in mind that some user organisations might want to use their own form or suggest amendments to the form.
- **Internal appointments**: Across the lead organisations in the initiative, all individuals who have access to private data of user organisations must be appointed as data processors. Server providers must also be sub-appointed by the data processors.

[4] Some national legal frameworks necessitate several different questionnaires.

Technical and contractual documents for user organisations

Both whistleblowing law and data protection regulations such as the GDPR require organisations implementing internal reporting mechanisms to adopt specific documents regulating how personal data is treated. Often, organisations are not equipped to draft all the relevant documents themselves, due to limited expertise or administrative and financial resources. It is therefore highly recommended that an initiative provides user organisations with guidelines, models and templates that they can adapt. This includes, for example, models for the privacy policy and the Data Protection Impact Assessment.

Certifications and qualifications

National legislation may require specific certification for secure reporting platforms. We suggest meeting criteria contained in ISO guidelines.[5]

Another recommended self-certification measure is inclusion in the Security Trust Assurance and Risk (STAR) registry, which encompasses key principles of transparency, rigorous auditing, cloud security and privacy best practices.

Additional national qualifications might be required to comply with a country's digital authority standards, and with the principle of "do no significant harm" . Where national whistleblowing authorities issue no specific certification, self-certification for compliance with national laws and by-laws helps users avoid inadvertent breaches.

We recommend that lead organisations organise a process similar to the one adopted for WhistleblowingIT, described below. If implementing a fully certified ISO 27001 procedure appears too demanding as a starting point, lead organisations can implement a self-assessed step-by-step procedure using the Cloud Security Alliance framework [6]

[5] ISO/IEC 27017: 2015 (Code of practice for information security controls applicable to the provision and use of cloud services) and ISO/IEC 27018: 2019 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

[6] https://cloudsecurityalliance.org/star/registry

The case of WhistleblowingIT

Taking into account the WhistleblowingIT set-up – the initiative is implemented by two partner organisations – the Italian legal framework, the European Whistleblowing Directive, the European GDPR and the ISO Standards, WhistleblowingIT adopted the following approach to comply with data protection standards:

- As lead for establishing overall data compliance, and as the contracting party with respect the user organisations, Whistleblowing Solutions took the following steps:[7]
    - Appointed an internal Data Protection Officer and formally communicated the appointment to the Italian Data Protection Authority. This step is typically necessary when dealing with a significant amount of data processing.[8]
    - Appointed TI Italy as sub-processor.
    - Appointed the data server provider as sub-processor, responsible for managing the infrastructure in a data-centre located in the EU, and specifically in Italy.
    - Issued a formal contract to each employee involved in the data processing, and specifically assigned to two employees the role of internal System Administrators, with full administrative access.
    - Created formal management procedures for data breaches.
    - Documented formal disaster recovery procedures, to ensure the quality of the process and minimise the possibility of data loss.

- Whistleblowing Solutions coordinated with TI Italy over the creation of a data processing agreement, so that the user organisations could formally authorise the two organisations to handle personal data processing on their behalf in adherence to GDPR.

- While creating these formal procedures, Whistleblowing Solutions:
    - Achieved ISO certification for the full process of digital whistleblowing provision based on GlobaLeaks[9]
    - Gained endorsement for the full process from the Agency for Digital Italy, responsible for listing software in the catalogue from which Italian public agencies must select the technologies they use. WBIT is listed as a SaaS The data server provider used in the project was specifically selected because listed in the catalogue.

The WBIT initiative created further complementary documentation to support user organisations, including:

- a template for the privacy policy regulating management of the whistleblowing data by the organisation;
- a collection of documentation and frequently asked questions about GlobaLeaks to simplify the understanding of the technology to end-users.

[7] In the WhistleblowingIT initiative, Whistleblowing Solutions is the only partner organisation with whom the user organisations enter into a contracting agreement.

[8] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[9] ISO 27001, ISO27017, ISO27018;

The Slovenian pilot, *Linija Spregovori!*

For the Slovenian whistleblowing initiative *Linija Spregovori!*, Transparency International Slovenia is the sole lead organisation. The chapter adopted the following approach:

- It appointed a Data Protection Officer and created a privacy policy, in compliance with national legislation, which will undergo a Data Protection Impact Assessment.
- It appointed its IT provider and data server provider as sub-processors.
- TI Slovenia requires user organisations to appoint it as an external data processor, using the template provided.
- The chapter also requires user organisations to sign a special agreement on data sub-processing by the IT providers. This document is not required by law, but follows the best practice in this field.

SUPPORTING EFFECTIVE WHISTLEBLOWING SYSTEMS

The broader aim of an initiative based on WBIT is to support the implementation of effective internal whistleblowing systems that are in line with legislation and best practice. An initiative should therefore provide relevant resources to user organisations.

RESOURCES ON INTERNAL WHISTLEBLOWING SYSTEMS

The initiative should provide the resources necessary to implement a whistleblowing system effectively. This includes:

- information on relevant national and European laws, regulations and official guidelines on whistleblower protection and data protection law
- key publications and guidelines on whistleblowing produced by relevant national and international actors. (See list of European and international resources in annex E.)

WhistleblowingIT also developed a model procedure for whistleblowing reports management, to assist user organisations in drafting internal procedures.

SUPPORTING COMMUNICATION OF THE INTERNAL WHISTLEBLOWING SYSTEM AND THE ONLINE CHANNEL

Information and communication measures are key to ensure that all employees and others entitled to use the organisation's internal channels are aware of its internal whistleblowing policy, procedures and available channels. Without proper information, potential whistleblowers might not know about the existence of the online whistleblowing channel or the internal whistleblowing system in general, or might lack the confidence to use the channel to report wrongdoing internally. Such information should be highly visible and accessible, via a wide range of media and communication channels.

Reminding organisations of this and providing templates for media and communication materials tailored to different audiences will help ensure that the organisations properly communicate their new online whistleblowing channel. User organisations may not know how to share information or who to share it with, and many have limited resources. Supporting them in this way contributes to achieving a whistleblowing initiative's primary aim, which is to promote best whistleblowing practice.

Annex D contains the following range of models and templates:

- A description of the online reporting platform for organisations to include in relevant internal policies and procedures, such as their whistleblowing procedure, and on their dedicated whistleblowing pages on their website and intranet. (Lead organisations should strongly encourage user organisations to have such dedicated pages.
- Model text for a news item on the organisation's website, intranet and newsletter, to inform audiences about the new tool adopted to strengthen the organisation's integrity and protect those who decide to report suspected wrongdoing.
- Model emails for different target audiences:
    - for personnel and collaborators (including shareholders, board members, volunteers and trainees)
    - for business partners, with whom the organisation has a past or existing contractual relationship, such as consultants, contractors, sub-contractors, suppliers and grantees.
- The initiative can also provide images for websites and posters the organisation can hang in its premises (see, for example, those provided by WhistleblowingIT).

Communications about the online reporting platform should always be accompanied by relevant information about a user organisation's whistleblowing and whistleblower protection policy and procedures. This could be through a link to the relevant section of its website, where personnel, collaborators and business partners can find information on:

- all the channels available to make a whistleblowing report, including the online reporting platform
- who can report, and what can be reported
- who qualifies for protection, and the types of protection and support measures provided by the organisation to whistleblowers (including procedures and remedies to address retaliation)
- confidentiality and anonymity (including legal exceptions and practical limitations)
- how the organisation will manage reports and communicate with the whistleblower, including how and when it will contact the whistleblower
- how personal data will be processed, how long it will be retained and for what purpose.

THE INITIATIVE WEBSITE

A website should be set up to host relevant information and resources such as:

- contractual and technical documentation, including related to privacy and data protection)
- resources and guidance to support the implementation of effective whistleblowing systems
- news on changes in relevant legislation and regulation (e.g. on whistleblower protection and data protection)

THE INITIATIVE TEAM: WHO SHOULD BE INVOLVED?

The initiative can be run by one lead organisation, with a team of internal and outsourced professionals with the required set of expertise. It can also be the result of a partnership between two or more organizations, each of them bringing different sets of expertise and resources to set-up and run the initiative.

Some of the required skills and expertise – such as IT, legal, design and, to some extent, communication – can be outsourced to consultants, volunteers and others, but it is important to note that the project management and whistleblowing expertise need to be internal to the lead organisations, given the importance of these skills for the effective implementation of the initiative and its credibility.

The WhistleblowingIT initiative was set up by two organisations, each with complementary roles:

- **Transparency International Italy** took on a management role, and brought its knowledge of whistleblowing law, regulations and best practices.
- **Whistleblowing Solutions Social Enterprise**, is the IT partner,[10] expert in SaaS provision in relation to the specific national and international legal framework.

Together, they contracted a provider for the data-centre where the system is hosted. WBS later acquired dedicated hardware resources in a data-centre run by an Italian IaaS provider, which simplified the privacy policy management significantly.[11]

When an initiative brings together several partners, they should clearly establish respective roles and responsibilities, and resource sharing – for example, who is taking on costs, and who is receiving payments. Where the initiative is run by one organisation, it must provide both the whistleblowing expertise and the management skills.

Different roles and expertise are needed to run an initiative:

[10] See the section on compliance with recommendations on the selection of the IT partner.

[11] The data centre provider needs to be formally included in the GDPR chain of data processing.

MANAGEMENT OF THE INITIATIVE

Tasks include the following:

- General management of available services
- Client relationship management, including interaction with existing user organisations and outreach to potential users.
- Financial management, including ensuring the financial sustainability of the initiative:
    - Designing a long-term sustainability model, including evaluating costs and setting offer pricing.
    - Finding seed financing, such as grants, to support the inception phase.
- Identify and coordinate with third parties to bring necessary expertise not covered by the lead organisations – for example, on data protection.
- Coordination with partners, external experts and providers, where their support and expertise are needed – for example, to develop or update documentation, or customise platforms.
- Basic tasks on the GlobaLeaks platform, such as account activations and configurations, or daily assistance on accessibility for user organisations, such as password changes. Staff will need to be trained on the use of the IT platform to carry out such tasks.

THE PROVISION OF WHISTLEBLOWING EXPERTISE

Responsibilities of the whistleblowing expert include:

- Production of guidance documents and other tools relating to the set-up and implementation of an effective whistleblowing system, in line with national law and best practices.
- Timely updates to the service to ensure compliance with legislation – for example, updating the questionnaires filled in by whistleblowers for their reports and documentation.
- Personal technical assistance and whistleblowing advice to users.

THE IT PROVIDER

The IT provider should have the following qualifications:

- Expert in Linux sysadmin, with knowledge of Ubuntu/Debian systems and SaaS experience.
- Expert in common web services management (web, mail, domain names, sites, forums services), including set-up, configuration, hardening and maintenance.

Preferably, they should also have ISO 27001, ISO 27017 and ISO 27018 certifications.

The IT partner or provider is responsible for the following:

- Setting up the fully operational digital platform:
    - Installing GlobaLeaks
    - Setting up a registration module enabling user organisations to sign up for the service with immediate activation via email.
- Ongoing support:
    - Ensure the operating system (Ubuntu/Debian) and the GlobaLeaks software are up to date, and maintain the operating system

    - Hold a quarterly meeting for updating skills of lead organisation staff in charge of management, addressing technical requests from organisations and flagging issues.
- Ad-hoc support:
    - Provide urgent technical assistance to organisations using the online reporting platform on specific issues, within 48 hours.
    - Setting up customised versions of the platform.

Ownership of data-centre

It is preferable that the IT partner or provider owns a data-centre where the data processing takes place and user organisations' data is stored.

Having the SaaS provider match the IaaS provider makes it possible to reduce and simplify the compliance costs. A qualified IaaS provider would probably already implement a full own GDPR chain and would be probably already ISO 9000 (quality) and ISO 27001/17/18 certified. Having additional certifications is preferable.

OTHER ROLES AND EXPERTISE NEEDED

If certain roles do not exist within the lead organisations, they could be outsourced to consultants or volunteers. These include:

- communication officer – to set up the website and prepare promotional materials
- designer – to design the logo and promotional materials
- Web developer – to set up the website
- Legal expert – to define and revise contracts and data protection policies and documents.

SETTING UP A GLOBALEAKS SOFTWARE AS A SERVICE (SAAS)

This section explains how to set up GlobaLeaks whistleblowing software as a service (SaaS), and gives an overview of relevant aspects to consider when planning, setting up and maintaining the initiative.

The section is not exhaustive and does not intend to replace specific manuals such as the GlobaLeaks official user guide and other manuals for the hardware and software technologies it mentions. These should remain the primary references.

INTRODUCTION TO GLOBALEAKS

GlobaLeaks is free, open-source software designed to enable anyone to easily set up and maintain a secure whistleblowing platform.

To fulfil its purpose, the software contains a set of configurations that are studied to be safe by design and by default for general implementation. Users are invited to change the configurations with care, and only if needed, and always keeping a track record of any change and the reason behind it.

Roles and threat modelling

GlobaLeaks rests on a clear design of roles and responsibilities to be assigned and fulfilled by different operators. Each operator's access to data is limited according to the specific tasks they need to perform to fulfil their role.

In the basic configuration of a GlobaLeaks platform, operators are divided into three groups:

- Whistleblowers: the individuals reporting malpractices through the platform, which is designed to optimise their user experience.
- Recipients: the individuals mandated to manage whistleblowers' reports.
- Administrators: The individuals configuring and running the GlobaLeaks platform. Administrators perform the maintenance and overall management of the platform, and provide technical assistance to recipients, but do not have access to whistleblowers' reports.

In the context of a SaaS system setup, user organisations' individual whistleblowing platform have this basic configuration. In addition, the lead organisation's administrators can configure all the user organisations' platforms.

HARDWARE AND SOFTWARE SELECTION

Hardware selection

GlobaLeaks is a self-contained technology optimized to reduce hardware requirements. This design choice, originally made to increase data privacy and maximise resilience to distributed denial-of-service means the platform can run on low-cost and widely available hardware.

Therefore, when selecting hardware, the IT provider is free to choose a technical infrastructure that best suits the needs of the initiative by balancing security and accessibility, without compromising either. Private technologies that are under the lead organisation's direct access and control offer the best solution, but only on the condition that the set-up is balanced overall and includes data and network redundancy in order to ensure a reasonable Service Level Agreement (SLA). This should inform the choice of the IaaS provider that will carry out the infrastructure management.

With a more complete and dedicated infrastructure, the IT provider can internalise other components of the initiative, such as web servers for public site implementation, the mail server used for communication, and other utility software used in the initiative. The use of open-source software can minimise the costs and security risks involved in using other third parties.

Examples of hardware infrastructure include:

Minimum: Virtual infrastructure hosted by an external IaaS Provider

- A virtual firewall on redundant infrastructure
- A virtual server on redundant infrastructure
- A backup solution on redundant infrastructure hosted in a different geographic location.

Best: Dedicated physical hardware infrastructure privately hosted by the lead organisation or IT provider or at an external IaaS Provider

- A cluster of two firewalls
- A cluster of two servers
- Network-attached storage (NAS)
- Redundant electricity line linked to two independent electric sources
- Redundant network line linked to two independent network operators
- A back-up solution on redundant infrastructure hosted in a remote location
- A replica of the hardware infrastructure in a remote high availability data-centre .

Software selection

GlobaLeaks is packaged for Debian/Linux and its official support is offered for any long-term supported (LTS) version of Debian and Ubuntu. The package includes all the software necessary to perform a full set-up without the need for additional software.

THE IT PROVIDER WILL NEED TO IMPLEMENT A MAIL SERVER OR SELECT A MAIL PROVIDER FOR THE NOTIFICATIONS E-MAILS SENT BY THE PLATFORM (E.G. TO NOTIFY USERS ABOUT THE RECEPTION OF WHISTLEBLOWING REPORTS).GLOBALEAKS SET-UP AND CONFIGURATION

This section details the main aspects involved in a technical set-up and configuration of the GlobaLeaks software.

The first software and configuration is typically executed by an IT provider. The subsequent steps can to be executed directly by the lead organisation.

Initial software set-up and configuration

For the initial GlobaLeaks software set-up, the IT provider should follow the official, up-to-date procedures.

The process consists of:

- a preliminary set-up of plain Debian or Ubuntu Linux system in LTS version
- downloading and running the official GlobaLeaks install script.

For the initial GlobaLeaks software configuration, the IT provider should run the official installation wizard that will guide them through a default software set-up. This will result in an initialisation of the software in the GlobaLeaks default configuration. The lead organisation then needs to configure it for the service set-up.

But first, the lead organisation's administrator must take a number of steps to ensure security and keys management.

Security and keys management

Managing a secure system where data is protected with encryption keys requires lead organisations to organise proper security of these keys. It is important that lead organisations understand that loss or compromission of authentication details and encryption keys may have a severe impact not only on the privacy of the information stored on the system, but also on the availability of that information. This is particularly critical in a SaaS initiative in which lead organisations have contractual obligations and responsibilities towards user organisations.

This section discusses the most important security operations for safely managing the service.

Account recovery keys

To enable users to recover access to their own account in case of loss of their password, the system implements an key recovery mechanism and make available to every user an account recovery Key. This measure ensures that users in possession of their own account recovery key can always restore their access to their own account and the data contained therein. The lead organisation's administrators should save their account recovery key at the first login after activating their account. They can access their account recovery key in the "Preferences" section. This is of particular importance for lead organisation's administrators, as they can restore account access to user organisations whose administrator have lost both their password and account recovery key, and therefore prevent data loss.

Two-factor authentication

After accessing their account recovery key, the lead organisation's administrator has to enable and configure two factor authentication (2FA) for extra security, For this, they need to install an authenticator app on their phone supporting the standard time-based one-time password (TOTP) protocol. Administrators may enable 2FA in the "Preferences" section.

The first administrator that sets up the platform can require other administrators of the lead organisation to set up the 2FA option, via the "Settings, Advanced" section .

Escrow keys

The GlobaLeaks software protects users' data via special encryption keys called "escrow keys" that enable authorised administrators to support users in changing or resetting passwords in case of password loss. Escrow keys are enabled by default, and the first administrator created during the initial application set-up can change users' passwords.

Secondary administrative accounts

To ensure that users' data is not lost due to human error, it is important that the lead organisation's primary administrator is backed up by at least one secondary administrator.

The primary administrator can create one or more secondary administrator and give them the privilege to change users' passwords. This important step is necessary to ensure that at least two users have access to escrow keys.

Configuration as SaaS

Once the lead organisation's administrator has taken the security and key management steps, they can configure the GlobaLeaks software as a service, by taking the following steps.

Domain name and securing web access

In order to host the online whistleblowing platform service on the web, the lead organisation's administrator must configure the site domain and secure web access by means of HTTPS. They can perform these configurations in the "Network" section.[12]

Name and brand

The administrator should configure the initiative's name and logo, and the text that will appear on the home page of the software – the page seen by organisations interested in becoming users- via the "Settings" page.

Creating different types of "standard" platforms

Lead organisations can decode to offer different types of standard whistleblowing platforms to user organisations that are best suited to their situation - for example a standard platform for public administrations and a standard platform for companies. This can be done for example by creating multiple specific questionnaires for the different types of platforms and defining which questionnaire should be automatically assigned to each platform generated.

Automatic generation of individual whistleblowing platforms

User organisations whistleblowing platforms can be generated manually or automatically. The lead organisation's administrator can enable the automated generation of platforms via the section "Sites - Options". Here, the administrator should:

- Enable the option "Allow users to sign-up";
- input the domain name that will be used for the service (e.g. whistleblowing.it). The GlobaLeaks software will automatically generate an individual site for the user organisation's whistleblowing platform on this domain (e.g. userorganisationname.whistleblowing.it);
- configure which of the questionnaires defined in the system should be automatically assigned to the automatically generated platform;
- Input the terms of service and the privacy policies that user organisations need to read and accept when signing up for the service.

Once the configuration is done, the landing page of the software will feature a sign-up form requesting new user organisations to provide relevant information about the organisation, to define the name of their individual platform site and to read and accept the terms of service and the privacy policy (see illustration below) Once this is done, their whistleblowing platform will be generated automatically.

It should be noted that it is not currently possible to generate automatically different types of platforms. If the lead organisation offers several types of standard platforms, they need to choose which type will be generated automatically – for example standard platforms for public administrations – and generate manually individual platforms for user organisations that need other types of standard platforms – for example for publicly-own companies and for private companies.

[12] Here, the administrator also has the option of securing the network connections by setting up a free Transport Layer Security (TLS) certificate by means of Let'sEncrypt technology.

WHISTLEBLOWINGPA

WhistleblowingPA - Registrazione

Registrazione

Nome *

Cognome *

Indirizzo email *

Indirizzo email (Conferma) *

Numero di telefono *

Organizzazione

Nome *

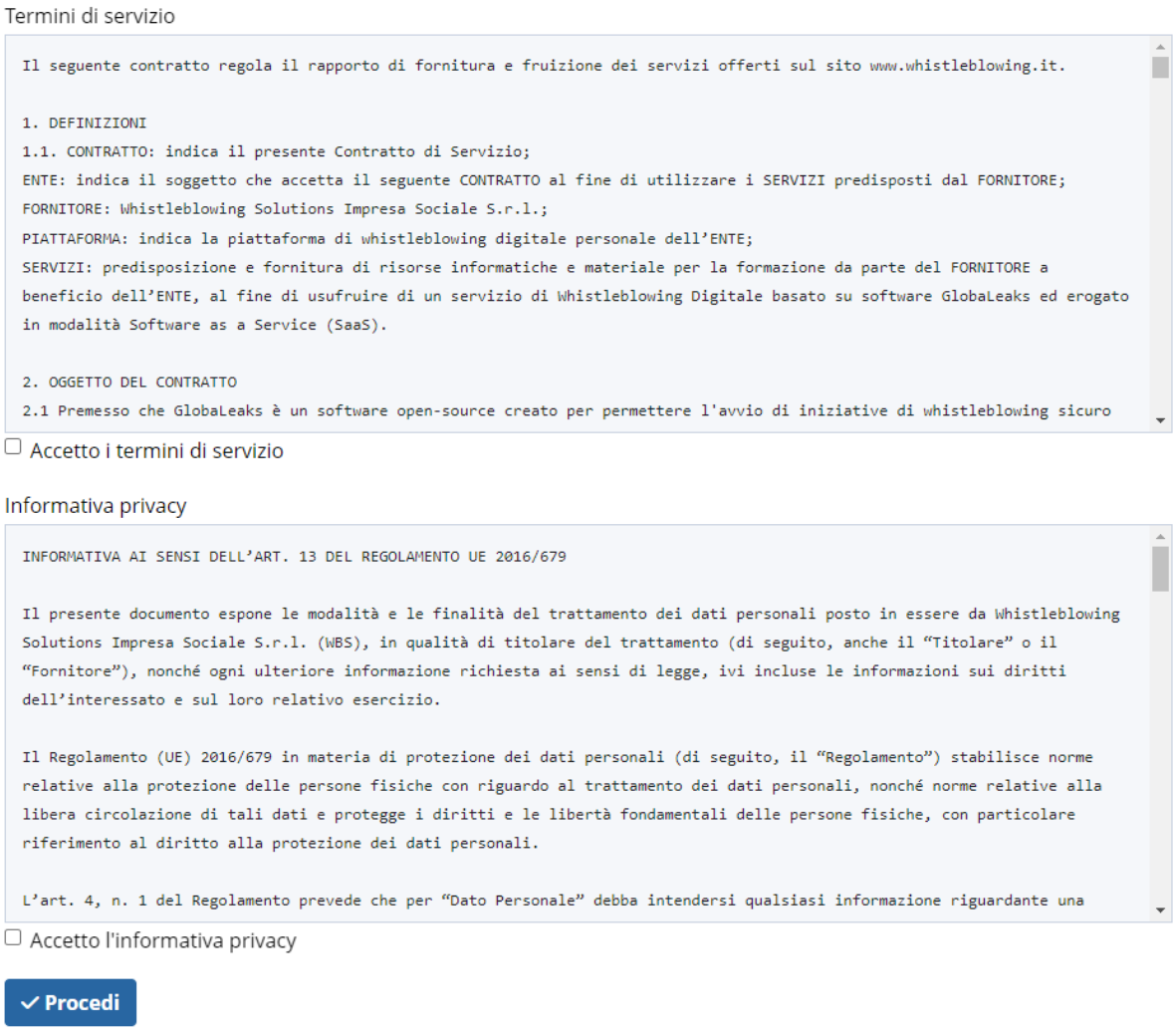
Indirizzo *

Codice fiscale *

Partita IVA *

Sito *

.whistleblowing.it



Mail notification server

By default, the software comes with a fully functional mail configuration, using the GlobaLeaks official mail servers. To implement a fully private set-up that includes only appointed data processors, the lead organisation should consider configuring the software to use private servers by specifying their SMTP configuration. This can be achieved via the Notification settings.

Mail notification templates

The platform provides a complete set of email notifications, including, for example, for platform activation and report notification, which can be customised in the "Notification" section of the platform.

ONCE THE INITIATIVE IS RUNNING

Generating and customising a user organisation's platform

User organisations' platforms can be generated and configure in the "Sites" section. In this section the lead organisation's administrators can:

- Create a new platform by indicating a platform name and clicking on "Add"
- Search for and access the platform of a user organisation in the sites list. The administrator can then customise that platform by clicking on the "Configure" button next to the name of that platform.

ANNEXES

A. USER GUIDES FOR GLOBALEAKS (FOR ADMINS, RECIPIENTS AND WHISTLEBLOWERS)

Guide to Using the GlobaLeaks Platform – Administrators

Guide to Using the GlobaLeaks Platform – Recipients

Guide to using the GlobaLeaks Platform - Whistleblowers

B. MODEL INSTRUCTION FOR ACTIVATION OF THE PLATFORM BY USERS

Once your registration is completed, you can activate your whistleblowing system yourself by following the steps described below.

Configurating the IT platform

Once your registration is complete, you have access to the administration portal of your online platform, where you will receive reports and can change the settings of your user profile.

To complete the configuration process, change the initial password given to you, check your user settings and report recipient details, and upload your organisation's logo. You will be able to access the portal whenever you want to check the reports received and to communicate with whistleblowers. Follow the instructions you received during registration to access the platform.

Appointing an external data processer

The online reporting platform involves the maintenance and updating of a cloud platform by [lead organisation IT provider (as appropriate)].

The organisation must therefore complete and sign the "Data processing agreement" that you received when registering, and send it to [email address created for GDPR purposes].

Publishing the reporting platform's web address and sharing the information

To start receiving reports, you should ensure that all potential whistleblowers are aware of the reporting platform, and have access to it. This includes the organisation's personnel, and other collaborators and business partners, such as contractors, sub-contractors, suppliers and their personnel, shareholders and board members, volunteers and trainees, as well as job applicants and bidders.

- **Signpost the web address for your new reporting platform (that we sent to you by email)**:
    - on your organisation's website and intranet, both on the homepage and the dedicated anti-corruption/whistleblowing pages
    - in your organisation's premises.
- **Spread the word about the reporting platform**:
    - Send a dedicated email to personnel, collaborators and business partners.
    - Make announcements at general staff meetings.
    - Publish a dedicated news item on your website and intranet, and in your internal and external newsletters.
- **Update relevant internal policies, procedures and other documents**
    - The adoption of [product name] to receive and manage whistleblowing reports might necessitate an update of your organisation's governance documents, including:
        - whistleblowing policy and procedures
        - anti-corruption policy
        - code of conduct
        - any other document that contains information on whistleblowing (such as employment and consultancy or suppliers contract templates).
    - You should also update your data protection policy to reflect the appointment of an external data processer, and publish the updated version.

Links to the online reporting platform, and all communication about it, should be accompanied by relevant information about your organisations' whistleblowing and whistleblower protection policy and procedures, including:

- all the channels available to make a whistleblowing report, including the [product name] online reporting platform
- who can report, and what can be reported
- who qualifies for protection and the types of protection and support measures provided by the organisation to whistleblowers (including procedures and remedies to address retaliation)
- confidentiality and anonymity measures (including legal exceptions and practical limitations)
- how the organisation will manage reports and communicate with the whistleblower (including how and when the whistleblower will be contacted)
- how personal data will be processed, how long it will be retained and for what purpose.

C. FAQ EXAMPLE

If my organisation joins the project by subscribing to the standard version, am I in compliance with [Name of national whistleblowing law]?

Yes. The law provides for the adoption of a reporting channel designed and established in a secure manner that ensures the confidentiality of the whistleblower and anyone mentioned in their report. [Name of product] does this, also providing a specially designed questionnaire.

Can I start using the standard version of the platform and then decide to customise it later?

Yes. An organisation can subscribe first to the standard offer and then easily change to a customised version without losing any data on its platform. The standard version is designed for all organisations that need a secure and dedicated tool. The customised version allows further improvement of the organisation's internal whistleblowing procedures, adapting the platform to the specific needs of the organisation.

How do I access technical assistance on the platform?

A forum is available for users of the free version of the platform, enabling exchange of information and opinions on its use and development. For paying users who decide to customise the IT platform, the initiative offers a dedicated assistance service.

Can the data entered during registration be changed later?

Yes. The replacement of the email address can be done directly by the user organisation on the platform. The other registration data is only relevant for registration purposes. During registration, it is necessary to have access to the email provided, as the configuration procedure requires verification of the email entered, and essential information will be sent to that email address.

If I want to know more about whistleblowing and organisations' legal obligations, can you help me?

The initiative seeks to help entities develop best practices for whistleblowing, alongside the online reporting platform. Materials are available in the resource section of this site and on the [name of lead organisation, with link] website to help organisations go beyond regulatory requirements and create effective internal whistleblowing systems.

Can I move the whistleblowing platform to my internal information systems after adopting [product name]?

Yes. [Product name] uses the GlobaLeaks whistleblowing software, which has no forms of lock-in or impediment sometimes applied in the commercial sphere. It is therefore possible to export and migrate your organisation's [product name] set-up to an installation of the GlobaLeaks software created independently on your own information systems. The GlobaLeaks software can be freely downloaded, modified and redistributed according to the AGPL 3.0 open-source licence from www.globaleaks.org and can be installed by an IT technician independently according to the instructions on the website.

Can I publish the platform link on an institution's intranet only?

No. The [name of national whistleblowing law] provides that former employees of the organisation, as well as employees and collaborators of suppliers and contractors, can also make reports, therefore the link must be published on the website.

D. MODEL COMMUNICATION RESOURCES FOR USER ORGANISATIONS

A range of material is available to help user organisations spread the word about their new online reporting platform.

Description of the online reporting platform

We suggest that user organisations include the description below of the online reporting platform in relevant internal policies and procedures, such as their whistleblowing procedure, and in the sections of their website and intranet dedicated to whistleblowing.

[Name of user organisation] has adopted [PRODUCT NAME], a safe online reporting platform provided by [Name of lead organisation]. Personnel, collaborators and business partners can report suspected wrongdoing encountered in a work-related context via this channel to [Name of user organisation].
Reporting through this new online platform offers many advantages for whistleblowers' safety and greater confidentiality:

The report is made by filling in a questionnaire and can be sent anonymously. The report can be made using any digital device (PC, tablet, smartphone) both from within the entity and outside it. The protection of anonymity is guaranteed in all circumstances.

The report is received and managed by the [title of the user organisation's employee responsible for handling reports], who has a duty of confidentiality.

The platform allows dialogue, even anonymously, between the reporting person and the [title of the user organisation's employee responsible for handling reports] for requests for clarification or further information, and feedback, without the need to provide personal contact details. At the time of sending the report, the whistleblower receives a 16-digit numeric code that they must keep in order to access the report again, read the response of the [title of the user organisation's employee responsible for handling reports] and communicate with them.

Reports can be sent to the web address [insert full address with link].

[Link / Button] Send a report

News item for user organisation's website, intranet and newsletters

[Name of user organisation] offers personnel and partners a new tool to fight corruption and other wrongdoing.

This is an online platform provided by [Name of lead organisation] that allows you to send to [Name of user organisation] reports about suspected wrongdoing encountered in a work-related context in a secure and confidential manner. The platform is open to all personnel, collaborators and business partners, including contractors, sub-contractors, suppliers and their personnel, shareholders and board members, volunteers, trainees, job applicants and bidders.

The main advantages of this tool include the opportunity to report suspected wrongdoing anonymously and to community with the person receiving the report, the [title of the responsible employee, such as Whistleblowing or Anti-corruption or Integrity officer] while remaining anonymous.

For more information on the organisation's whistleblowing and whistleblower protection policy and procedures, and to send a report, click here [link to the dedicated whistleblowing/integrity/ anti-corruption page]. For more information on [PRODUCT NAME], visit the [INSERT URL] website.

Model emails

Personnel and collaborators

Email to personnel and collaborators (including shareholders, board members, volunteers and trainees) to tell them that the organisation has adopted [PRODUCT NAME] and that they can now use a safe, confidential online platform to report wrongdoing internally.

Sender: Head of the user organisation
CC: Person responsible for the user organisation's internal whistleblowing system
Subject: Safe online platform available for internal reporting (whistleblowing)

Dear colleagues and collaborators,

Whistleblowing is one of the most effective ways to detect and address wrongdoing, helping to protect our organisation and the public from the damaging effects of misconduct. To enable our personnel, collaborators and business partners (including shareholders, board members, volunteers and trainees) to report wrongdoing they encounter in a work-related context, [entity name] has implemented an internal whistleblowing system since [date].

[User organisation name] has now adopted [PRODUCT NAME], a safe, confidential online whistleblowing channel provided by [lead organisation name], which you can use to report suspected wrongdoing to [Entity name].

Reporting through this new online platform offers greater confidentiality and many advantages for whistleblowers' safety:

- A report is made by filling in a questionnaire and can be sent anonymously.
- The report is received and managed by the [title of the organisation's employee responsible for handling reports], who has a duty of confidentiality.
- The platform allows dialogue between the reporting person and the [title of the user organisation's employee responsible for handling reports] even anonymously, enabling requests for clarification or further information, and feedback, without the need to provide personal contacts. When a whistleblower sends a report, they receive a 16-digit numeric code, which they must keep in order to access the report again, read the response of the [title of the user organisation's employee responsible for handling reports] and communicate with them.
- The report can be made from any digital device (PC, tablet or smartphone), both from within the entity and outside it. The protection of anonymity is guaranteed in all circumstances.

For more information on the organisation's whistleblowing and whistleblower protection policy and procedures, and to send a report, click here [link to the dedicated whistleblowing/integrity/ anti-corruption page].

For more information on [PRODUCT NAME], visit the [INSERT URL] website.

Business partners

Email to all organisations with whom the user organisation has a past or existing contractual relationship – such as consultants, contractors, sub-contractors, suppliers and grantees – to tell them that that they and their personnel, collaborators and relevant business partners can now use a safe online platform to report wrongdoing committed in, by or for [Entity name].

Sender: Contact person for the business partner at [entity name]
CC: Person responsible for the organisation's internal whistleblowing system
Subject: Safe online platform available to report wrongdoing to [entity name]

Dear company / supplier,

By virtue of [the existing or recently concluded] working relationship with our organisation, we wish to inform you of a new development in our whistleblowing policy and procedures, which may also concern you / your company.

Whistleblowing is one of the most effective ways to detect and address wrongdoing, helping protect our organisation and the public from the damaging effects of misconduct. To enable our business partners and their personnel and collaborators (contractors, sub-contractors, suppliers and their personnel) to report wrongdoing they encounter in a work-related context, [entity name] has implemented an internal whistleblowing system since [date].

[Entity name] has adopted [PRODUCT NAME], a safe, confidential online whistleblowing channel provided by [lead organisation name]. You / your organisation's personnel and contractors can now use this channel to report suspected wrongdoing committed in, by or for [Entity name] directly to us.

We strongly encourage you to disseminate this information to your workers, collaborators and relevant business workers.

Reporting through this new online platform offers greater confidentiality and many advantages for whistleblowers' safety:

- Anyone can make a report by filling in a questionnaire, which can be sent anonymously.
- The report is received and managed by the [title of the user organisation's employee responsible for handling reports], who has a duty of confidentiality.
- The platform allows dialogue between the reporting person and the [title of the organisation's employee responsible for handling reports], even anonymously, enabling requests for clarification or further information, and feedback, without the need to provide personal contacts. At the time of sending the report, the whistleblower receives a 16-digit numeric code that they must keep in order to access the report again, read the response of the [title of the organisation's employee responsible for handling reports] and communicate with them.
- The report can be made from any digital device (PC, tablet or smartphone), both from within the entity and outside it. The protection of anonymity is guaranteed in all circumstances.

For more information on [user organisation]'s whistleblowing and whistleblower protection policy and procedures, and to send a report, click here [link to the dedicated whistleblowing/integrity/anti-corruption page].

For more information on [PRODUCT NAME], visit the [INSERT URL] website.
We thank you for your cooperation.

E. RESOURCES TO SUPPORT THE IMPLEMENTATION OF EFFECTIVE INTERNAL WHISTLEBLOWING SYSTEMS

Transparency International resources

Internal whistleblowing systems: Best practice principles for public and private organisations (2022).

The Business Case for "Speaking Up": How Internal Reporting Mechanisms Strengthen Private-Sector Organisations (2017).

Overview of whistleblowing software (2020).

Gender Sensitivity in Corruption Reporting and Whistleblowing (2020).

Financial incentives for whistleblowers (2018).

Internal Whistleblowing Mechanisms – Topic Guide (2017).

10 Anti-Corruption Principles for State-Owned Enterprises (2017).

Other resources

International Chamber of Commerce – Guideline on Whistleblowing (2022).

International Organization for Standardization (ISO) – Whistleblowing management systems – Guidelines, ISO 37002:2021.

UNODC – Speak Up for Health! Guidelines to enable whistle-blower protection in the health-care sector (2021).

Eurocadres – Guide to Internal Whistleblowing Channels and the Role of Trade Unions (2021).

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

European Data Protection Supervisor – Guidelines on processing personal information within a whistleblowing procedure (2016).