E.A.T.

EXPANDING ANONYMOUS TIPPING

· THE HANDBOOK ·

Co-funded by the
Internal Security Fund
of the European Union

"This E.A.T. handbook was funded by the European Union's Internal Security Fund — Police."
"The content of this E.A.T. handbook represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains."

· SUMMARY ·

· INTRODUCTION ·

E.A.T. (Widely Expanding Anonymous Tipping Technology Deployment, Operation, and Trustworthiness to Combat Corruption in Eastern and Southern Europe)
is a two-year project funded by the European Commission.
The project will create anonymous whistleblowing mechanisms (using the GlobaLeaks system) to channel reports to public and private sector entities in 11 EU countries.

This document is designed to provide guidance to all those who receive disclosures through their participation in the EAT project. Most often this will be compliance officers associated with EAT beneficiary organisations, but recipients may also include EAT partners or media organisations. An explanation of the different submission models used in the EAT project is supplied in the Appendix.

As framework of this recommendation, we considered the new European Directive on whistleblowing protection and the ISO 37002 on Whistleblowing Management Systems as fundamental benchmarks.

THINGS TO CONSIDER

1. RESPECT ANONYMITY WHEN IT IS REQUESTED

The whistleblowing platforms set up as part of the EAT project give reporting persons the option to provide complete, partial or no personally identifying information.

Where a whistleblower wishes to stay anonymous, we recommend that initial investigations be undertaken without identifying information being required or stored.

Once a whistleblower has confidence that an investigation is being undertaken in a way that protects his confidentiality minimizing the risks to duffer retaliation themselves, they may be more comfortable in sharing identifying information.

Ways of producing confidence include a progress feedback status of an investigation to the whistleblower and being clear about when they can expect to receive further news.

The new EU Whistleblower Directive makes stipulations about investigation procedures and timelines that should be regarded as a baseline standard.

7 days - confirmation of receiving the submission
90 days sending out the proposal on further steps - offering solution – request for extra information

2. RECOGNISE THE COSTS AND RISKS OF WHISTLEBLOWING FOR THE WHISTLEBLOWER AND MITIGATE THEM IN THE WAY THEIR REPORT IS INVESTIGATED

Retaliation is a real threat for many whistleblowers. Investigative procedures must be designed and implemented so to minimise these risks, whether the whistleblower's identity is known or not.

Measures that may be taken include excluding those in or likely to be in a working relationship with the reporting person, and any who are implicated in a report, from having any role in the investigation of that report.

The EU Whistleblower Directive sets down standards for confidentiality and record-keeping that should be abided by.

3. VERIFY MATERIAL BASED ON THE VALUE OF THE INFORMATION, NOT ON YOUR VIEW OF THE ATTITUDES OR OPINIONS OF THE WHISTLEBLOWERS

It is important to judge reports received on their merits. In the final analysis, it is the quality and verifiability of the information supplied that is most important.

Assessing the motivation of the source is important only insofar as it assists in judging the veracity of a report.

It may well be the case that verification requires additional information. Be aware that the whistleblower may not have access to this information themselves, or may feel that disclosing this information puts them at risk.

In such cases, where a whistleblower may not have or want to reveal his access to information, he may be able to assist those investigating by letting them know where information is located.

4. ESCALATE CONCERNS TO REGULATORS AND OTHER AUTHORITIES WHERE APPROPRIATE

Some issues for which reports may be received carry with them obligations to pass concerns on to regulators or other authorities.

We encourage partners and beneficiaries to involve regulatory and other authorities where it is appropriate to do so.

One of the least-heard whistleblowing stories is that where concerns have been received and successfully resolved because proper reporting channels are available. We encourage the discussion of successful case studies that have come about through the EAT project.

5. SECURELY DELETE DATA WHEN NECESSARY IN ACCORDANCE WITH EAT POLICY

Whistleblowing reports often include personally identifying data, both of the reporting person and potentially those who are the subject of the report.

While the preservation of this data will be required for a certain time in order to make sure that reports are adequately investigated, material should eventually be deleted in accordance with data protection standards.

EAT partners will publish policies for the treatment of this personally identifying data and other content and metadata involved in the EAT project.

6. UNDERSTAND THE RELEVANT LEGAL FRAMEWORKS AND INTERNATIONAL STANDARDS GOVERNING INTERNAL DISCLOSURES

We encourage all project partners to become familiar with the key international standards in this area. That includes in particular the new EU Whistleblower Directive and the guidelines for ISO 37002 on Whistleblowing Management Systems.

7. SHARE THE RIGHT INFORMATION ON THE REPORTING PROCESS AND RECOMMENDATIONS ON HOW TO PROTECT THE DATA.

Employees and other persons who may want to share information internally have to understand how they are expected to proceed. EAT partners recommend to make available a clear guide to make disclosures, including specification related to data treatment and anonymization.

THINGS TO HAVE IN MIND POSSIBLE RISKS AND CONSEQUENCES

When submitting sensitive information, you must consider the risks related with taking that action in revealing the truth, as you may be subject to retaliation by parties that do not like what you have to say.

That is why you must take all possible actions to preserve your anonymity.

You need to be aware of the social impact and technical risks, and take the right countermeasures to protect yourself. The most applicable protection strategies depend on the scenario, especially those related to social risks.

1. SOCIAL RISK

Before submitting any information you should consider what will happen "after" the information has been sent and when the news about the facts related to the info you submitted reaches public media attention.

Ask yourself the following questions to understand your real risk context:

- Do people other than you have access to the information you are going to submit?
- If the submitted information will reach public attention, does someone will ask you something about it?
- Are you really willing and ready to cope with all the "stress" of an internal or external investigation (someone asking you about something) about the submission?
- Are you ready to handle possible negative publicity based on misinformation and online abuses?

You should consider submitting to a GlobaLeaks site only after a full understanding and deep reflection on the previously illustrated points.

2. MINIMISING SOCIAL RISK

From a social protection perspective, you should try to take precautions like the following:

- Before you make a submission, don't tell your intention to anyone

- After you make a submission, don't tell what you have done to anyone
- After the news about the submission gets out to public media, be really careful in expressing your opinion about it with anyone
- Be sure that there's no surveillance systems (cameras or other) in the place where you acquire and submit the information
- Don't look around on search engines or news media website for the information you submitted (this would reveal that you knew about it earlier)
- Consider the possibility that your family, friends or close colleagues may be under risk as well.

These are recommendations you might consider in order to reduce social impact.

3. TECHNOLOGICAL RISKS

You must be aware of the fact that while using a computer and the internet to exchange information, most of the actions you do leave traces (computer logs) that could lead an investigator to identify where you are and who you are.

For this reason you must consider risk mitigation strategies and adopt very specific precautions to avoid leaving technological traces about your doing.

You may leave computer's traces while:

- Researching the information to be submitted
- Acquiring the information to be submitted
- Reading this web page
- Submitting the information to us
- Exchanging data with receivers of your submission

All these actions may leave traces that compromise your security, but with a few technological protection steps, you can minimize the risks.

4. TECHNOLOGICAL PROTECTION

The complexity of today's computing and network systems means that fully understanding the technological risks associated with submitting a disclosure can be difficult.

While no technology can offer a 100% guarantee of security, there are recognised procedures for mitigating the risks.

However, by strictly following the procedures and tips reported below, you should be safe enough:

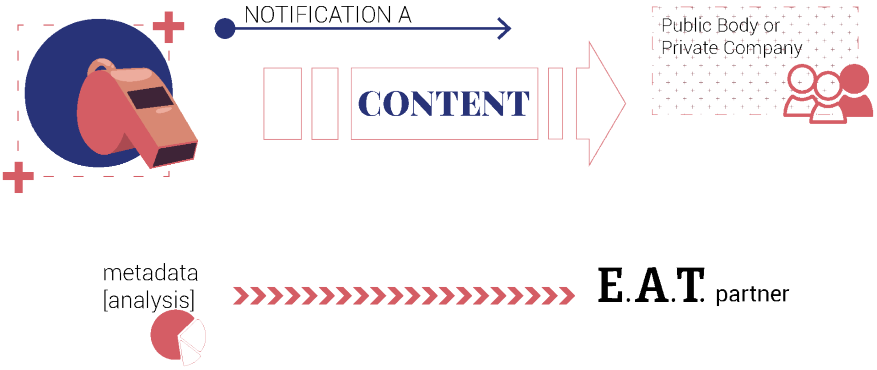
- Submit information using Anonymous Web Browsing software **Tor Browser Bundle** (it's easy, use it!)
- Don't submit information from the personal computer provided to you by your employer (consider using a spare one)
- Keep the receipt of your submission safe and destroy this information when you don't need it anymore
- Don't keep a copy of the information you submitted
- While acquiring the information to be submitted, try to ensure that you are not leaving a trail that could lead back to you (eg: if you use files on a USB key to make a submission, delete those files after making your submission and fill the device with innocuous files)
- Be aware of the fact that "**metadata information**" may be present in some of the data you are submitting.
- Consider converting all the data that you are sending us into standard PDF format.

EAT SUBMISSION MODELS

We are leaving it up to our partner organisations to decide which of a small number of submission models they wish to employ. The vast majority of the dropboxes will be operating on submission model A. A small number of our partner organisations, who have more experience in managing dropboxes, have expressed an interest in using submission model B, which involves notifications to multiple parties, and even data being sent to multiple parties. It is also possible that a small number of these dropboxes may employ model C, where EAT will provide a parallel dropbox which involves a media organisation rather than a public or private sector entity.

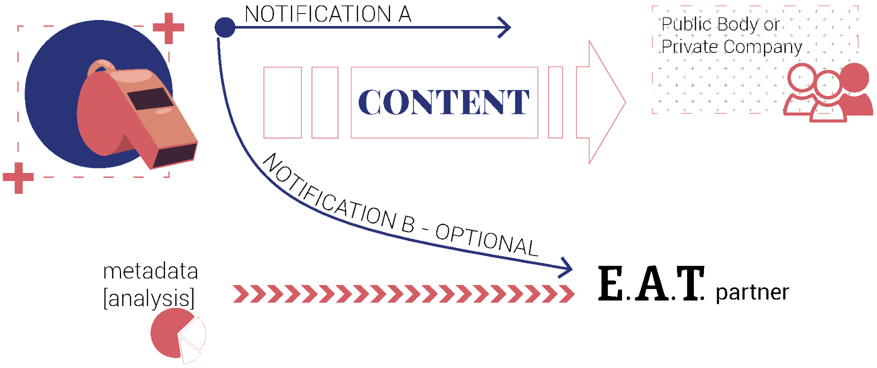
MODEL A

In model A, the dropbox is associated with a public or private sector entity and whistleblowers are encouraged to submit reports relating to that beneficiary entity. The dropbox itself will be operated by Hermes, but the beneficiary entity will have access to particular administrative functions. Submitted disclosures are sent to an officer of the beneficiary organisation. Certain kinds of metadata will be recorded by Hermes and analysed by Blueprint for Free Speech.



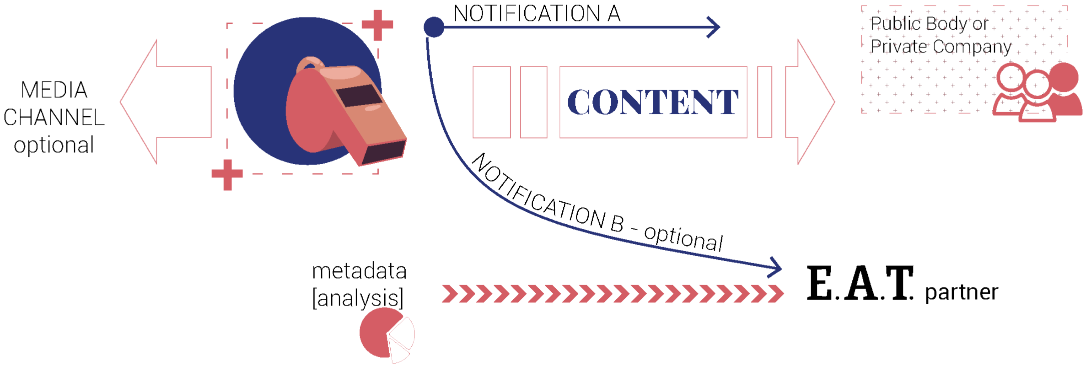
MODEL B

In model B, the whistleblower is given a choice about whether they would like to submit their report to the beneficiary, sending a notification only to the responsible at beneficiary ends, or to both the beneficiary responsible and the EAT partner responsible. Some EAT partners will allow the reporting person to send the data also to them, if the reporting person decides to make a submission to the beneficiary and the NGO. Certain kinds of metadata will be recorded by Hermes and analysed by Blueprint for Free Speech.



MODEL C

In model C, the beneficiaries will be able to adopt model A or B. However, EAT project will provide an external and parallel channel associated with a media organization. The dropbox itself will be operated by Hermes, but the media organisation will have access to particular administrative functions. Submitted disclosures are sent to a journalist working for the media organisation. Certain kinds of metadata will be recorded by Hermes and analysed by Blueprint for Free Speech.



· NOTES ·

Co-funded by the
Internal Security Fund
of the European Union

"This E.A.T. handbook was funded by the European Union's Internal Security Fund — Police."
"The content of this E.A.T. handbook represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains."