Search. Observe. Protect.

EU and UK whistleblowing policy

Introduction

Elastic recognizes the importance of the integrity of our business practices and financial information and is committed to fostering a transparent corporate culture. We maintain this Policy to promote and encourage all of our employees and others who reasonably believe that they are aware of any suspected wrongdoing to report such matters without fear of harassment, discrimination, or retaliation.

This policy is applicable to all Elastic companies located within the European Union and United Kingdom and is intended to facilitate compliance with the EU Directive n°2019/1937 of October 23rd, 2019 (we refer to this document as the EU Whistleblowing Directive). This policy applies subject to specific requirements provided by national rules and regulations, which are listed in an appendix dedicated to each concerned country.

This Policy sets out the categories of matters that must be reported, how to report them, the procedure that is followed once a report has been made, and how employees reporting concerns are protected.

1. Purpose and Scope

❖ **What are the matters concerned?**

Any past, present, or likely future wrongdoing will fall within this Policy if it concerns one or more of the following categories:

- Questionable accounting, internal accounting controls, or auditing matters;
- Criminal offenses, including but not limited to fraud, bribery, and corruption;
- Any other failure to comply with any applicable national laws, rules, or regulations or the EU Whistleblowing Directive, including those related to public procurement, money laundering, security of network and information systems, and protection of the financial interests of the EU and/or internal market;
- Failure to comply with Elastic's Code of Business Conduct and Ethics;
- Failure to comply with any of Elastic's published corporate policies, including our compliance policies addressing anti-bribery, export control, trade sanctions, data security, data privacy, insider trading, and similar compliance matters; or
- Covering up the wrongdoing in any of the above categories.

❖ **Who is covered by the policy?**

This Policy applies to Elastic's operations in the EU and to all of its directors, officers, members of administrative, management or supervisory bodies, including non-executive members, and employees, and trainees located in the EU. It also applies to Elastic's customers, vendors, contractors, subcontractors, suppliers, and any persons working under their supervision located in the EU, who reasonably believe that they have information about suspected wrongdoing.

It applies before, during and after any contractual relationship with Elastic, including when the relationship has ended or has not yet begun when the information was obtained during the recruitment process or other pre-contractual negotiations.

We refer to all people covered by this Policy as "Elasticians".

2. Policy Statement

This Policy has been established to enable all Elasticians to confidentially and anonymously submit complaints related to any of the foregoing misconduct.

It is Elastic's corporate policy to encourage all of its employees, directors, and officers to promptly bring to the company's attention all suspected wrongdoing under this Policy. It takes courage to make a report, but you have Elastic's unwavering commitment to protect against any reprisal anyone who reasonably believes to have information about suspected wrongdoing and who has in good faith reported a complaint, or who assists in any related investigation. We will not engage in, and will not tolerate any of the following: threats, disciplinary measures, discrimination, harassment, retribution, retaliation, harm to your reputation (particularly in social media), financial loss (including loss of business and loss of income), blacklisting on the basis of a sector or industry-wide informal or formal agreement that may prevent you from finding employment in the sector or industry in the future, early termination or cancellation of a contract for goods or services, cancellation of a license or permit, or psychological or medical referrals.

This protection applies to any Elastician who had reasonable grounds to believe that the information on breaches reported was true at the time of reporting.

This protection also applies to "facilitators", i.e., third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context (colleagues, relatives, etc.) and legal entities that the reporting persons own or for which they work for or are otherwise connected with in a work-related context.

If you believe you are or have been experiencing negative consequences for having submitted a complaint or for participating in a related investigation, please report this immediately, following the guidelines set forth in the "How to Report" section below. Elastic will promptly and thoroughly investigate your complaint, and if any claim of any type of reprisal mentioned above is substantiated, then we will take appropriate action, up to and including terminating the employment of those engaged in such behavior.

It is Elastic's corporate policy to seriously consider all complaints and to investigate them appropriately. We will bring each complaint to a conclusion and will respect to the fullest extent practicable the confidentiality of each person who reports, except as necessary to conduct the investigation and take any remedial action, and in accordance with and as permitted by applicable laws.

While we strongly encourage Elasticians to report in good faith any wrongdoing that this Policy covers, we must warn you that deliberately filing a complaint with false information, providing false information during an investigation into a complaint, or refusing to cooperate with an investigation, will all be grounds for disciplinary action, up to and including termination of employment or any other working relationship with Elastic. Subject to local laws and regulations, this may also result in civil, criminal, or regulatory liability. Also, if you report misconduct in which you have had personal involvement, the fact that you make the report does not exempt you from possible disciplinary actions or civil, criminal, or regulatory liability. However, Elastic's disciplinary actions will take into consideration that an employee has voluntarily reported the suspicions of misconduct.

3. How to Report

If you have observed or are otherwise aware of potential violations of this Policy, and if you reasonably believe the violations are of the nature described under "Purpose and Scope" above, we encourage you to promptly take one of the following steps:

- Discuss the situation with your manager;
- If your manager is involved in the situation or you are uncomfortable speaking with your manager, send an email to ethics@elastic.co or contact the Chief Ethics & Compliance Officer, Senior Vice President of Human Resources, General Counsel, or Chief Financial Officer. You will find all of these individuals' contact information on our Wiki pages dedicated to ethics and compliance;
- If the actual or suspected misconduct or irregularity pertains to an executive director of Elastic, report concerns directly to the Lead Independent Director of Elastic at the company's registered office at Keizersgracht 281, 1016 ED Amsterdam, the Netherlands;

- Anyone (including employees, contingent workers, vendors, and all others) may also report ethical, legal, or regulatory concerns via the Ethics and Compliance Hotline by phone or via the web-reporting tool available at https://www.elastic.co/about/trust;

- In addition, if your complaint relates to accounting, internal controls or auditing matters, you may contact the Chairperson of our Audit Committee by sending an email to ethics@elastic.co or by writing to Elastic N.V., 800 West El Camino Real, Suite 350, Mountain View, California 94040, Attn: Chairperson of Audit Committee. We will forward all such communications to the Chairperson of our Audit Committee.

Employees can also consult Elastic's Chief Ethics & Compliance Officer in confidence about suspicions of possibly reportable misconduct. The contact information for the Chief Ethics & Compliance Officer is available on our Wiki pages dedicated to ethics and compliance. If requested by the employee, the Chief Ethics & Compliance Officer will escalate the matter by submitting a formal report. Additionally, you always have a right to contact law enforcement, regulatory authorities or any other external channel provided by national law, and nothing in this Policy limits any Elastician from making a good faith report or complaint to the appropriate authorities. We encourage you to report through one of the Elastic's channels prior to making external complaint if the concern can be addressed internally, unless you consider doing so would trigger a serious risk of retaliation despite the protections provided by this Policy. Finally, please note that you may also make public disclosure:

- after reporting the matter to Elastic or to the authorities, if no appropriate measures were taken in response to your report within the timeframe mentioned in section 4 below, or
- if you have reasonable grounds to believe that:
    - the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or
    - as it relates to external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

4. Investigations and Corrective Actions

The non-executive directors of Elastic have overall responsibility for monitoring Elastic's responses to all received complaints. In cases where allegations are made against members of the Board of Directors of Elastic, the non-executive members of the Board can choose to initiate and coordinate their own investigation.

Investigation into all accounting, internal controls and auditing complaints will be overseen by the Audit Committee of the Board of Directors and are handled as directed by the Audit Committee in accordance with internal procedures. The Audit Committee will also investigate (or designate others to conduct or manage the investigation while overseeing their work) and determine appropriate disciplinary action with respect to any complaints that implicate any executive officer of Elastic.

All other complaints will be handled as follows. After a complaint is received, Elastic will acknowledge receipt within seven days. We will then route the complaint to the appropriate professionals to comprehensively review and resolve the matter reported in the complaint. For example, depending on the nature of a complaint, it may be addressed by Human Resources, the Chief Ethics & Compliance Officer, or other seasoned professionals.

We are committed to dealing with all genuine concerns in a fair and appropriate way. We will take corrective action in any particular case that will depend on the nature and gravity of the conduct or circumstances reported and the results of the investigation. The corrective action will be proportionate to the seriousness of the offense and may include disciplinary measures against the accused party, up to and including termination of employment or any other working relationship that the offending party may have with Elastic. We will also take reasonable and necessary steps to prevent the occurrence of any similar issues in the future.

Within three months after acknowledging receipt of the report, we will advise each reporter as to how Elastic will deal with the complaint, the expected timeframe of the investigation, and the results of the investigation and the specific resolution (so long as we are able to disclose this information). However, due to confidentiality obligations and privacy and other considerations, there may be times when we will not be able to provide the specific details regarding the investigation or any resulting corrective or disciplinary action that was taken. Any information shared with the employee about the investigation and action taken must be treated as confidential information by the employee.

5. Whistleblower Protection Programs

Elastic will not in any way limit or prohibit you from filing a charge or complaint with, or otherwise communicating or cooperating with or participating in any investigation or proceeding that may be conducted by, any national, federal, state, or local government agency or commission. You may disclose documents or other information to such government agencies, as permitted by law, without giving notice to, or receiving authorization from, Elastic. However, you should take reasonable precautions to prevent the unauthorized use or disclosure of any confidential or proprietary information of Elastic to any parties other than the applicable government agency, and you should not disclose any Elastic attorney-client privileged communications or attorney work product. None of the agreements that you entered into with Elastic, or any of the policies to which you are subject, should be interpreted or understood to conflict with this Policy.

6. Confidentiality and Data Privacy

We will ensure confidentiality and will not reveal your identity at any point without your consent, unless there is a necessary and proportionate obligation under EU or national law in the context of investigations by authorities or judicial proceedings, in particular to safeguard the rights of defense of persons concerned.

All data collected under this policy will be treated in compliance with the requirements of the European General Regulation on the Protection of Personal Data of 27 April 2016. Please see Appendix 1 and our corporate privacy policy for more information on your data protection rights and how Elastic processes your personal data.

7. Amendment

We are committed to periodically reviewing and updating this Policy to reflect the changing legal and business environment.

Appendix 1: Compliance of report retention with GDPR requirement

❖ Automated Data Processing

The whistleblowing procedure in Elastic's EU Whistleblowing Policy is subject to the implementation of an automated processing of reports that meets the requirements of the European General Regulation on the Protection of Personal Data (GDPR) of 27 April 2016.

❖ Data Collected

During the investigation period, the person who collects the data must ensure that only information that is relevant and necessary for the purposes of the processing operation is collected and/or stored in the registration system.

The only persons who will have access to the personal data processed in the context of the whistleblowing are:

- The people specially in charge of whistleblowing report within Elastic;
- The persons directly responsible for the investigation of reports and/or those directly involved in the decision making on the follow-up to the report;
- The referent or service provider in charge of collecting and processing the report. The referent or service provider undertakes, by contract, not to use the data for purposes other than report processing, to ensure their confidentiality, to respect the limited data retention period and to destroy or return all manual or computerized personal data carriers at the end of its service.

❖ Data Retention and Security Measures

The person in charge of processing the report shall take all appropriate measures to preserve the security of the data throughout the period of processing and storage of such data.

If it appears the report does not fall within the scope of the EU Whistleblowing Policy, and/or if no follow-up action is taken, the data relating to the report shall be destroyed or made anonymous without delay, and at the latest within two months of the closure of the investigation.

Where disciplinary measures or legal proceedings are implemented against a defendant or the author of an abusive alert, the data relating to the alert may be stored until the end of the proceedings or the limitation period for appeals against the decision.

The data collected may be stored in the form of an intermediate archive for the purpose of protecting the whistleblower and to enable continuous infringements to be established. This storage period must be strictly limited to the purposes pursued, determined in advance and brought to the attention of the data subjects.

Anonymized data may be stored for an unlimited period of time.

❖ Impact Assessment

The present reporting procedure was subject to an impact assessment which did not allow the characterization of residual risks.

❖ Privacy Policy

The whistleblower and the person(s) concerned by the report may access, upon request to the person in charge of processing the report, the data concerning them and request their rectification or deletion if they are inaccurate, incomplete, equivocal or out of date.

The right of rectification may be exercised only to rectify factual data, the material accuracy of which can be verified by the person in charge on the basis of supporting evidence, without erasing or replacing even erroneous data originally collected.

In the event of data transfer outside the European Union, Elastic will take the necessary measures to guarantee the protection of personal data, in compliance with the provisions applicable to the GDPR.

Appendix 2 : Specific requirements for France

The current applicable law in France is the Sapin II law n°2016-1691 of December 9, 2016 relating to transparency, the fight against corruption and the modernization of economic life. This Appendix 2 contains provisions that provide additional rights and protections to Elasticians based in France which are available under Sapin II. It will be periodically updated to reflect the changing legal and business environment in France.

1. Purpose and Scope

In addition to the protections in the EU Whistleblowing Directive and the Policy, employees of Elastic based in France (including interns, temporary employees or employees of a temping agency assigned to Elastic) (we refer to such persons in this Appendix 2 as French employees) will benefit from the statutory protections offered under Sapin II if the subject matter of a report concerns any of the following matters:

a. a crime or illegal act,
b. a serious and clear breach of an international engagement ratified or approved by France, or of a unilateral act of an international organization based on such an engagement,
c. a serious and clear breach of the law or regulation,
d. a threat or serious prejudice for general public interest, or
e. moral and sexual harassment, violence at work, sexist behavior or discrimination.

2. Policy Statement

N/A

3. How to Report

French employees will benefit from the statutory protections offered under Sapin II if they report observing the following priority order:

a. Unless there is a serious and imminent danger or a risk of irreversible damage, the report must first be made through one of the Elastic channels listed in the bullet points in section 3 of the Policy.
b. In the absence of action by one of the Elastic channels within three months from the date of receipt of the alert, the alert may be sent, if the author of the alert deems it necessary, to the judicial authority, the administrative authority or the professional bodies concerned, as appropriate.

c. Only if one of the abovementioned public bodies fails to deal with the alert within three months after receiving it, the whistleblower may decide to make public disclosure if the whistleblower considers it appropriate.

In addition, in order to benefit from the statutory protections offered under Sapin II, French employees must:

a. have personal knowledge of the reported facts,
b. act in good faith, i.e., do not raise an alert with the aim of harming others,
c. act in a disinterested manner, i.e., without benefiting or seeking to benefit from an advantage or remuneration in return for the report, and
d. make a disclosure in a manner that is necessary and proportionate to safeguard the interests involved.

4. Investigations and Corrective Actions

Elastic will inform the person implicated:

- of the alleged misconduct he/she is being investigated for, to be able to exercise his rights of defense; and
- of his/her rights to access and rectification of his/her personal data, as mentioned in Appendix 1.

Elastic will make this notification within a reasonable time and taking into consideration the interests of the investigation and mandatory legal requirements in France.

5. Confidentiality

Throughout the processing of the report, Elastic will also take all reasonable measures to guarantee confidentiality of the identity of the person targeted by the report and the nature of the facts reported.

Elements likely to identify the person against whom an alert has been issued may not be disclosed, except to the judicial authority, until it has been established that the alert is well-founded.

Appendix 3 : Specific requirements for The Netherlands

The current applicable law in the Netherlands is the House for Whistleblowers Act (*Huis voor Klokkenluiders)*. This Appendix 3 contains provisions that provide additional rights and protections to Elasticians based in the Netherlands which are available under the Whistleblowers Act. It will be periodically updated to reflect the changing legal and business environment in the Netherlands.

1. Purpose and Scope

The protections of the Whistleblowers Act extend to all individuals who have (or have had) an employment contract with Elastic and all individuals who otherwise carry out (or have carried out) work for the company. Therefore, the Whistleblowers Act applies not only to employees and former employees but also to trainees, volunteers, and independent contractors.

2. Policy Statement

N/A

3. How to Report

Under the Whistleblowers Act, employees are expected to report their concerns internally. Special Dutch rules apply regarding exceptional circumstances where the following "suspicions involving the public interest" can be reported to the House for Whistleblowers:

- suspicions that are based on reasonable grounds, arising from knowledge acquired by the employee while working for the Company or arising from knowledge acquired by the employee through work activities within another company or organization; and which
- involve the public interest because of the violation of laws and regulations, or threats to public health, the safety of individuals, the environment or the proper functioning of a public service or a company as a result of improper actions.

External reporting of these "suspicions involving the public interest" could be appropriate if an internal report was not adequately followed up by the Company, or if the employee cannot reasonably be required to first submit an internal report, for instance because of a legal reporting obligation, a present danger resulting in an important and urgent public interest, or a legitimate fear for retaliation. If an external report is to be made, it should be to a competent regulator and in an appropriate manner taking into consideration the legitimate interests of all involved. Except in these rare

circumstances, reporting matters to the press or on social media will not be appropriate or permissible and any employee will be at the risk of breaching the duty of confidentiality and forfeiting legal protection.

Given the possible severe consequences of external reporting, employees are encouraged to seek, in confidence, advice from Elastic's Chief Ethics & Compliance Officer before reporting any concern outside Elastic (please consult our Wiki pages dedicated to ethics and compliance for contact information). You can also consult the advisory department (*afdeling advies*) of the House for Whistleblowers. For more information regarding the House for Whistleblowers and its procedures, please see https://huisvoorklokkenluiders.nl/.

4. Investigations and Corrective Actions

N/A

5. Confidentiality

An employee can request that their report should be treated confidentially. The name of the employee who submitted a report in good faith shall not be disclosed to others within or outside Elastic, unless the employee gives their prior written consent or Elastic is required to comply with a legal or regulatory obligation. The employee is entitled to deny or withdraw their consent at any time and shall be informed of this right prior to giving consent.

Exceptions to confidentiality may be reasonably necessary in circumstances including, but not limited to, disclosure necessary to facilitate the investigation, take any remedial action, and to comply with applicable law. Access to reports and records of complaints may be granted to regulatory agencies and other parties if required by applicable law at the discretion of the non-executive directors. However, the name of the employee will not be disclosed unless the employee has given its consent or there is a legal or regulatory obligation to do so.

Appendix 4: Specific requirements for the UK

The current applicable law in the UK is the Public Interest Disclosure Act 1998 (PIDA), which inserted various new sections into the Employment Rights Act 1996. The purpose of PIDA is to encourage the disclosure of information that is in the public interest, such as illegal, dangerous, or corrupt practices. This Appendix 4 contains provisions that provide additional rights and protections to Elasticians based in the UK which are available under PIDA. It will be periodically updated to reflect the changing legal and business environment in the UK.

1. Purpose and Scope

In addition to the protections in the EU Whistleblowing Directive and the Policy, employees of Elastic based in the UK, including consultants who undertake to provide work personally and contract workers and agency workers assigned to Elastic (we refer to such persons in this Appendix 4 as UK employees), will benefit from the statutory protections offered under PIDA if the disclosure tends to show one or more of the following kinds of malpractice, regardless of whether the malpractice occurs in the UK:

a. the commission of a criminal offence,
b. breach of legal obligations,
c. a miscarriage of justice,
d. the endangerment of the health and safety of any individual,
e. environmental damage, or
f. the deliberate concealment of information relating to any of the above.

2. Policy Statement

N/A

3. How to Report

For a disclosure to be protected under PIDA, the following requirements must be met:

a. a UK employee making a disclosure of information must have a reasonable belief that one or more of the above-mentioned acts of malpractice has occurred (i.e., there must be identifiable objective grounds to justify the belief) and that the allegations are substantially true;
b. the belief itself must be reasonable in all circumstances to make the disclosure; and

c. the UK employee must believe that making a disclosure is in the public interest and not for personal gain.

Although a UK employee acting purely in self-interest will not be protected under PIDA, if s/he makes a disclosure about a breach of individual rights (e.g., employment rights), the UK employee may still be protected even if the disclosure is in his/her self-interest.

PIDA protects UK employees that make disclosures in bad faith, so long as the other requirements for protected disclosures are met. However, the amount of compensation received by a UK employee making a disclosure in bad faith disclosure may be reduced up to 25%.

In most cases, UK employees will make a disclosure to their employer, and PIDA is drafted to encourage such internal disclosures. However, if a UK employee is making an external disclosure (for example to colleagues, a trade union, another employer, a regulator, a professional body, or the media), the following additional requirements must be met to be protected under PIDA:

- the UK employee making the disclosure, reasonably believes s/he will be subjected to a detriment by the employer if s/he would disclose to the employer;
- there is no prescribed regulator, and the UK employee making the disclosure reasonably believes that evidence will be destroyed if s/he would disclose to the employer;
- the UK employee making the disclosure has previously made a similar disclosure to the employer or a prescribed person; or
- the relevant wrongdoing is exceptionally serious.

In addition, a UK employee making a disclosure to a regulator must also reasonably believe that the malpractice falls within that regulatory body's jurisdiction and that the allegations are substantially true. And with respect to a disclosure to the media, a UK employee must also ensure that the disclosure is reasonable in all the circumstances and not made by for personal gain. The "reasonableness" requirement may be difficult to satisfy if the UK employee has not approached the employer first and given the employer an opportunity to rectify the problem.

4. Investigations and Corrective Actions

N/A

5. Confidentiality

Any provision in an agreement is void under PIDA if it purports to prevent a UK employee from making a protected disclosure. For this reason, confidentiality clauses in employment contracts are subject to the overriding right to make a protected disclosure. In addition, non-disclosure provisions in settlement agreements, including those conciliated via the Advisory, Conciliation and Arbitration Service, will be void if they purport to preclude a UK employee from making a protected disclosure.