Breach notification policy

Public

27 September 2024

Version 3

Together for better connections

wengage

Inhoud

Roles and responsibilities

Role	Description	Name / Title
R	**Responsible**: The person who performs the activity/work to achieve the task.	Legal Counsel
A	**Accountable**: The person who must ensure the task is completed as required. Can delegate the work to those responsible.	CHRO
C	**Consulted**: Those whose opinions are sought, typically subject matter experts and with whom there is a two-way communication.	HR, Legal
I	**Informed**: Those who are kept up to date on progress, often only on completion of the task or deliverable and with whom there is a one-way communication.	Employees

Version

This document is updated when necessary, but reviewed at least every year.

Version	Author	Approvals	Date	Description
1	CHRO	Excom, Legal	03/03/2023	Publication
2	Legal	Excom, HR	27/09/2024	Alignment with Code of Conduct

Purpose

WEngage and its entities, (hereinafter referred to as "the Company") is committed to acting with integrity and ethics in its operations. This policy has been adopted in accordance with the Belgian law of 28 November 2022 on the protection of reporting breaches of Union or national law established within a legal entity in the private sector, which implements the European 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, hereinafter referred to as "the Act".

It is often the company's own employees who are the first to know about threats or breaches that occur within a company. However, they could be prevented from expressing their concerns or suspicions for fear of reaction or reprisals. However, these fears could ultimately prevent the Company from taking the necessary steps to address these breaches.

On the one hand, the purpose of this policy is to report **any breach, illegal, unethical or fraudulent activity** related to the Company's activities without fear of sanctions or other measures.
On the other hand, the purpose of this policy is to **receive and investigate violations of the Code of Conduct** in a similar manner, where appropriate with appropriate protections as provided by law.

The purpose of this policy is to:

- enable the confidential, anonymous or non-anonymous, reporting of information on possible or actual breaches;
- provide protection to persons who report a breach or assist the reporting person;
- lay down the procedure to be followed by the person reporting a breach for that purpose.

This policy is available on the Company's website (wengage.eu), on the internal communication channels and may be amended from time to time.

Important: Of course, this policy does not in any way exclude the direct dialogue and communication of information outside the reporting procedure. The Company would like to emphasize that employees with concerns or suspicions can always contact their immediate supervisors, confidential advisors, the Human Resources department or the Compliance department.

Scope

Who is covered by this policy?

This policy applies to the following individuals:

- current and former employees, who are or were related under an employment contract with the Company;
- candidates who are or were involved in a recruitment procedure in the Company;
- persons who work or have worked on a self-employed basis with the Company and the candidates for an independent cooperation in the context of pre-contractual negotiations;
- volunteers and trainees (paid or unpaid);
- shareholders and members of the administrative, management or supervisory body of the Company (including non-executive members);
- any person who works or has worked under the supervision and direction of contractors, subcontractors and/or suppliers of the Company;
- any person who has information about breaches in the Company in the areas of financial services, products and markets, even outside of a work-related context.

Which violations need to be reported?

Infringements as defined in the Act must be reported if they relate to one of the following areas:

- Public procurement
- Financial services, products and markets, prevention of money laundering and terrorist financing;
- Product safety and compliance,
- Transport safety,
- Protection of the environment,
- Radiation protection and nuclear safety,
- Food and feed safety, animal health and welfare,
- Public health
- Consumer protection
- Protection of privacy and personal data, and security of network and information systems,
- Fight against tax fraud,
- Combating social fraud,
- Complaints about child labour – forced labour.

In addition, infringements that may affect the financial interests of the European Union can be reported, as well as infringements related to the European internal market, including Union rules on competition and state aid.

Infringement is defined as an act or omission which is unlawful or contrary to the purpose or application of the rules in the above-mentioned areas. It concerns any infringement of the legal or regulatory provisions in this regard or the provisions taken in implementation of the aforementioned provisions.

Violations as described in the Code of Conduct must be reported:

- Misuse of customer data
- Corruption

- Extortion
- Breach of professional secrecy
- Interest taking and misappropriation
- Fraud
- Assault on the honour or good name of persons
- Crimes and misdemeanours against the security of the state

The notification

Purpose of the report

Any infringement in relation to the areas referred to in paragraph 2.2 as well as any information relating to such infringements, including any reasonable suspicion of actual or potential breaches that have occurred or are very likely to occur within the Company, and attempts to conceal such breaches within the Company, may be notified in writing or orally through any of the channels referred to in paragraph 4.

The conditions for notification and protection

The report must be made in good faith and must not be based on mere rumors or gossip, nor must the report be intended to cause harm to the Company.

The reporting person must have reasonable grounds to believe that the information about the violations was true at the time of the report.

Where the report contains false, unsubstantiated or opportunistic allegations, or is made solely for the purpose of harming or harming others, the Company may take appropriate disciplinary and/or judicial measures against the reporting person, including the imposition of sanctions in accordance with the Company's work regulations.

Notification channels

Any person covered by this policy who has information about actual or suspected infringements referred to in point 2.2 is encouraged to report it to the Company as soon as possible in good faith and in accordance with the principles set out in point 3.2.

What channels are available?

A breach can be reported through one of the following channels:

- Via the intranet: www.wengage.info
- Via internet: wengage.eu/nl-be/juridisch
- Per e-mail: legal@wengage.eu

The report should preferably be made in Dutch, French or English. Any report that is made in another language will first have to be translated as this may affect the accuracy of the content of the report.

These reporting channels are accessible at all times, 24 hours a day, 7 days a week.

It is also possible to request a face-to-face meeting with a Reporting Administrator as listed below in Section 4.3.1 of this Policy.

Each of the above-mentioned channels is managed in a confidential and secure manner to ensure the confidentiality of the identity of the reporting person and any third parties named in the report. Access to the channels is strictly limited to employees who have access to them based on responsibilities and/or authority.

How does the notification proceed?

A report shall include a brief description of the reasonable suspicions about a committed or potential breach of one of the criteria set out in point 2.2. domains that have taken place or are very likely to take place, as well as any attempts to conceal or conceal such infringements.

At the discretion of the reporter, the report can be made anonymously or by filling in a digital form.

The Company does not encourage reports in an anonymous manner, as this prevents the Company from properly investigating and handling the report. However, if the reporter does not feel comfortable, the reporter can of course choose to remain anonymous. The Company will, of course, respect this choice of the reporter and an anonymous report will be taken as seriously as a non-anonymous report.

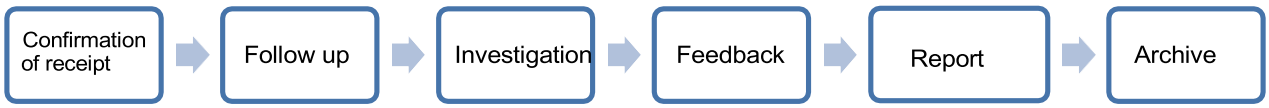
In the case of anonymous reports, the Company will be confronted with certain limitations in the follow-up of the report. For example, it may not be possible for the Company to:

- acknowledge receipt of the report to the reporting person;
- investigate your report further, as the Company may not be able to contact the reporter with a view to obtaining additional information. It is therefore important that the reporting person provides sufficient information so that this information can be properly investigated;
- provide feedback on the outcome of the study;
- proactively monitor any retaliation.

The report must be sufficiently detailed and documented and must include the following information (where the relevant information is known):

- a detailed description of the events and how they came to the attention of the reporter;
- the date and place of the event;
- the names and functions of the persons concerned, or information enabling them to be identified;
- the names of other persons, if any, who may corroborate the facts reported;
- when making a report, the name of the reporter (this information is not requested when an anonymous report can be made); and
- any other information or elements that may help the investigation team to verify the facts.

What happens after the report?



Confirmation of receipt

The author of the report will receive an acknowledgement of receipt within 7 days of notification. A file number is also provided for the purpose of following up the file.

Follow up

Follow-up refers to any action taken by the recipient of a report to verify the accuracy of the allegations made in the report and to address the reported breach if necessary, including through measures such as an internal preliminary investigation, investigation, prosecution, recovery of funds or termination of proceedings.

The report manager follows up on reports, maintains communication with the reporter, requests additional information if necessary, provides feedback to the reporter and receives any new reports.

Investigation

The report administrator can decide whether or not to investigate a report after consulting with management within the organization.

The report will be promptly and carefully investigated in accordance with this policy. All investigations are conducted thoroughly in accordance with the principles of confidentiality, impartiality and fairness to all persons involved. The report administrator shall set up an investigation team if necessary. The investigation team will be empowered in accordance with the existing policies within the company.

Persons involved in the (potential) breaches reported by the reporting person will be excluded from the investigation team and will not be allowed to participate in the assessment of the report or the determination of the actions to be taken in relation to the report.

Conflicts of interest are reported to the Board of Directors if the Executive Board/Executive Board is targeted in the report. If the board of directors appears to be involved, the general meeting of the Company will be informed.

Feedback

The reporting administrator shall provide appropriate feedback to the reporting person within a reasonable period of time, and no more than three months from the date of acknowledgement of receipt of the report. This feedback shall include information for the reporting person about the measures planned and/or taken and the reasons for these measures. They inform the reporter via the chosen internal reporting channel.

Report

At the end of the investigation, the investigation team will draw up an overview report, describing the investigative measures carried out. An edited, non-confidential and anonymized version of this review report may be shared with local or executive management outside of the investigation team on a need-to-know basis only in order to reach a final decision.

A member of the investigation team prepares a final report describing the facts and the final decision:

In the event that the (potential) breach is demonstrated, relevant actions will be determined for the purpose of countering the (potential) breach and protecting the Company; or
In the event that the investigation shows that there is insufficient or no evidence of the (possible) breach, no further action will be taken.

The reporter will be informed about the closure of the report and the decision taken via the internal reporting channel of his/her choice.

The Notification Administrators

The Company's notification administrators are:

- Bert Nijs, WEngage Legal Counsel
- Juan Alleman, Lawyer

Each reporting administrator carries out his/her task independently and without conflict of interest. They are subject to a duty of confidentiality.

Archive

The Company shall keep a record of all reports received, in accordance with the confidentiality measures set out in Section 5.1 of this Policy.

These reports and the information related to them will be kept for as long as the contractual relationship between the reporting person and the Company is ongoing.

Where, with the consent of the reporter, a call-recorded telephone line or other voice messaging system with call recording is used for reporting, the Company shall record the verbal report as follows:

- by a recording of the conversation in a sustainable and retrievable form; or
- by a complete and accurate written record of the conversation prepared by the notification administrator. The reporter will be given the opportunity to check, correct and sign for approval of this written statement.

If a non-recorded telephone line or other non-recorded voice messaging system is used for the notification, the Company will record the verbal report in the form of an accurate record of the call drawn up by the staff member responsible for handling the report. The reporting person will be given the opportunity to check, correct and sign this report.

In the event of a face-to-face meeting with the reporting manager, a complete and accurate record of the maintenance will be kept in a durable and retrievable form, subject to the reporter's consent. The Company has the right to register the maintenance as follows:

- by means of a call recording in a durable and retrievable form;
- by an accurate record of the maintenance. The reporting person will be given the opportunity to check, correct and sign this report.

External messaging channel

Reporting persons may use an external reporting channel after reporting through the internal channels or directly through the external reporting channels if they deem this more appropriate.

The Federal Coordinator is entrusted by the Belgian legislator with the coordination of reports submitted through external channels. A Royal Decree is being drafted in which the task of the Federal Coordinator is assigned to the Federal Ombudsman.

The Federal Coordinator is responsible for receiving external reports, checking their admissibility and forwarding them to the competent authority for investigation, which will be different depending on the subject of the report.

This authority may be, for example, the FPS Policy & Support (in the field of public procurement), the Financial Services and Markets Authority (FSMA), the National Bank of Belgium (NBB) or the Supervisory Board of Auditors (in the field of financial services, products and markets), the FPS Economy (in the field of consumer protection), the Data Protection Authority (in the field of the protection of privacy and personal data), etc.

In exceptional cases, the Federal Coordinator may also conduct the investigation on the merits.
The contact details of the Federal Coordinator are as follows (subject to the entry into force of the Royal Decree):

Address:	Leuvenseweg 48 bus 6, 1000 Brussel
Online complaint:	https://www.federaalombudsman.be/nl/klachten/dien-een-klacht-in
E-mail address:	contact@federaalombudsman.be
Telephone:	0800 99 961
Fax:	02 289 27 28

Safeguards

The Company undertakes to make every effort to provide appropriate and effective protection to the persons covered by this policy, insofar as the report complies with the conditions of the Act, in particular by taking the following measures:

Guarantee of confidentiality

The Company warrants to take the necessary measures to ensure that employees and other persons targeted by this policy can file a report with the Company in complete confidence.

The Company undertakes to put in place the necessary measures to ensure that the identity of the reporting person cannot be disclosed to persons other than the staff members authorised to receive or follow up on reports without his free and explicit consent.

This also applies to any information from which the identity of the reporting person can be deduced, directly or indirectly.

By way of derogation from the previous paragraph, the identity of the person reporting the infringement may be disclosed where this is necessary and proportionate under special legislation in the context of an investigation by national authorities or in the context of legal proceedings, in particular to protect the rights of defence of the person concerned.

In the latter case, the reporting person shall be informed of the disclosure of his or her identity before it takes place, unless such information would jeopardise ongoing investigations or legal proceedings. This is the case, for example, if the reporting person represents an important witness in court or in the event of an unjustified or unlawful report in order to protect the rights of defence of the person concerned.

Protection against retaliation

Any form of retaliation against the persons referred to in point 2.1 who are protected under this policy, including threats of retaliation and attempted retaliation, shall be prohibited, in particular in the following forms:

- suspension, temporary decommissioning, dismissal or similar measures
- relegation or refusal of promotion;
- change of position, change of workplace, reduction of pay, change of working hours;
- Suspension of or refusal of training
- negative performance assessment or reference;
- the imposition or application of any disciplinary measure, reprimand or other sanction, including a financial penalty;
- coercion, intimidation, bullying or exclusion;
- discrimination, disadvantageous or unequal treatment;
- failure to convert a fixed-term employment contract into an employment contract of indefinite duration, even though the employee had a legitimate expectation that he would be offered an employment contract for an indefinite period;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including reputational damage, particularly on social media, or financial loss, including loss of revenue and revenue;
- Blacklisting on the basis of an informal or formal agreement for an entire sector or industry, preventing the reporting person from finding employment in the sector or industry;
- early termination or cancellation of a contract for the supply of goods or services;
- revocation of a license or permit;
- psychiatric or medical referrals.

Processing of personal data

Within the framework of the internal reporting procedure, the Company is considered to be the controller of the personal data.

Any processing of personal data under this policy is carried out in accordance with the applicable legislation on the protection of personal data, including the European General Data Protection Regulation ("GDPR").

The following personal data may be processed in the context of a report: name, position, date of employment, contact details and email address of the reporting person and of persons involved in the breach, any identified or identifiable information provided by the reporting person and collected in the context of the internal investigation. This processing of data is carried out in the context of compliance with a legal obligation and/or the legitimate interest of the Company, to the extent that the internal reporting channel exceeds the legal objectives, in particular the detection of breaches, the guarantee of the security and ethical conduct of the Company.

Personal data that is clearly not relevant to the processing of a report will not be collected or, if collected, deleted as soon as possible. These records shall be kept until the infringement reported is time-barred and, in any event, for a period of five years after the notification.

The identity of the reporting person can only be disclosed with the consent of the reporting person. Other data will also remain strictly confidential and will only be shared on a strict need-to-know basis.

All persons whose personal data are processed in the context of breach notifications have the right to access and copy, the right to rectification, the right to erasure, the right to object and the right to lodge a complaint with the supervisory authority in accordance with the applicable law. However, these rights may be limited by the rights and freedoms of others, in particular the reporter's right to confidentiality and the Company's right to proper follow-up of the report.

For more information on the processing of personal data, please refer to the Privacy Notices for Employees, Job Applicants, Independent Service Providers and Temporary Workers and the Privacy Policy available on the Company's internal communication channels.

The Company reserves the right to change this policy at any time, including but not limited to changes in relevant legislation and/or operational needs.