Breach notification Policy

---

1. Purpose

WEngage and its entities, (hereinafter referred to as "the Company") intends to act with integrity and ethics in its operations, and therefore wishes to ensure that its employees have the opportunity, in accordance with the modalities and conditions, to report in the Company any observed or suspected breaches of the legal and regulatory standards referred to in article 2.2 of this policy, in the most serene and confidential manner.

It is often in-house employees who are the first to know about threats or breaches occurring within a company. However, they might be stopped from voicing their concerns or suspicions for fear of reactions or reprisals.

However, this potential fear could ultimately result in the Company being kept in the dark about possible breaches and unable to take the necessary steps to address them. This would therefore harm the interests of the Company, which pursues high standards of good governance and professional ethics.

The purpose of this policy is to prevent this situation by strongly encouraging all employees and other individuals who have a contractual relationship with the Company, to report any breach, illegal, unethical, or fraudulent activity related to the Company's business without fear of sanctions or other action.

This policy was adopted in accordance with the Act of 28 November 2022 on the protection of notifiers of breaches of Union or national law established within a legal entity in the private sector, thereby implementing the European Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of individuals notifying breaches of Union law, hereinafter referred to as "the Act".

The purpose of this policy is to:

- enable the confidential, anonymous or otherwise, notification of information about potential or actual breaches enable;
- provide protection to individuals, notifying a breach or assisting the notifier;
- establish the procedure to be followed by the notifier of a breach for this purpose.

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

This policy obviously in no way excludes direct dialogue and communication of information, outside the notifying procedure. The Company wishes to emphasize that employees with concerns or suspicions may at any time address their immediate superiors, the Human Resources Department or the Compliance Department.

2. Scope

2.1 Who is covered by this policy?

This policy applies to the following individuals:

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

2.2 Which breaches can be notified?

Only breaches relating to any of the following areas as defined in the Act can be notified:

- Public procurement,
- Financial services, products and markets, prevention of money laundering and terrorist financing;
- Product safety and product compliance,
- Transport safety,
- Protection of the environment,
- Radiation protection and nuclear safety,
- Safety of food, 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,
- Fight against social fraud,
- Complaints on child labour - forced labour.

In addition, breaches which could harm the financial interests of the European Union can be notified as well as violations, relating to the European internal market including the Union rules on competition and state aid.

A violation means the act or omission that is unlawful or contrary to the purpose or application of the rules in the areas mentioned above. It refers to any violation of the legal or regulatory provisions on the matter or the provisions taken in implementation of the previously mentioned provisions.

3. The notification

3.1 Purpose of the notification

Any breach relating to the areas referred to in article 2.2 as well as any information about such breaches, 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 article 4.

3.2 The conditions of a notification and protection

The notification must be made in good faith and must not be based on mere hearsay or gossip nor must the aim be to harm the Company.

The notifier must have reasonable grounds to believe that the information about the violations at the time of the notification was true.

If the notification contains false, unsubstantiated or opportunistic allegations, or is made solely for the purpose of disadvantaging or harming others, the Company may take appropriate disciplinary and/or judicial measures against the notifier, including the imposition of sanctions in accordance to the employment regulations of the Company.

4. Notification channels

Any individual covered by this policy who has information about actual or suspected breaches referred to in article 2.2 is encouraged to notify it in good faith and in accordance with the principles set out in article 3.2 to notify it to the Company.

4.1 Which channels are available

A notification of a breach can be made through one of the following channels:

- Via the intranet: www.wengage.info/articles/beleid-omtrent-het-melden-van-inbreuken
- Via the Internet: https://wengage.eu/nl-be/juridisch
- By e-mail: legal@wengage.eu

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

These notification 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 notification manager as mentioned below in article 4.3.1 of this policy.

Each of the above channels is managed in a confidential and secure manner so the confidentiality of the identity of the notifier and any third parties named in the notification, are guaranteed.
The access to the channels is strictly limited to employees who have access to them, based on responsibilities and/or authorisations.

4.2 How does the notification proceed?

A notification includes a brief description of the reasonable suspicions about a committed or possible breach of one of the domains mentioned in article 2.2, that has occurred or is highly likely to occur as well as about any attempts to conceal or disguise such breaches.

The notification can be made anonymously or not, at the option of the notifier, by completing a digital form.

The Company does not encourage notification in an anonymous manner, as this prevents the Company from properly investigating and dealing with the notifier to be properly investigated and dealt with. However, if the notifier would still not feel comfortable, the notifier can of course choose to remain anonymous. The Company will of course respect this choice of the notifier and an anonymous notification will be taken as seriously as a non-anonymous notification.

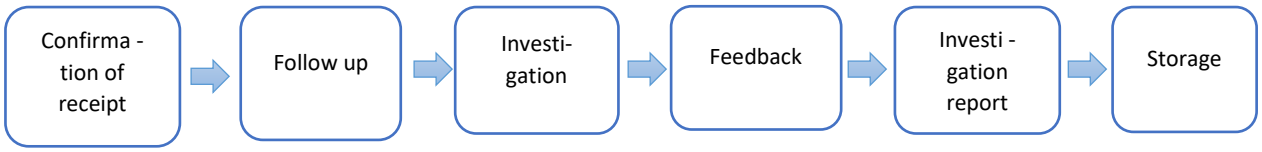
In case of anonymous notification, the Company will face certain restrictions in the follow-up of the notification. For example, it may not be possible for the Company to:

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

The notification should be sufficiently detailed and documented and should include the following information (when the relevant information is known):

- a detailed description of the events and how they came to the attention of the notifier;
- the date and place of the event;
- the names and positions of the people involved, or information enabling their identification;
- the names of other people, if any, who can corroborate the facts notified;
- when making a notification, the name of the notifier (this information is not requested when an anonymous notification can be made); and
- any other information or elements that may help the investigation team to verify the facts.

4.3 What happens after the notification?



1-Confirmation of Receipt
The author of the notification will receive an acknowledgement of receipt within 7 days of notification. A file number for the purpose of following up the file.

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

The notification manager follows up on notifications, maintains communication with the notifier, requests additional information, if necessary, provides feedback to the notifier and takes in any new notifications.

3-Investigation
The notification manager may decide whether or not to investigate a notification after consulting with management within the organization.

The notification will be investigated promptly and carefully in accordance to this policy. All investigations will be thoroughly conducted in accordance with the principles of confidentiality, impartiality and fairness towards all people involved. The notification manager will establish an investigation team, if necessary. The investigation team is given authority in accordance with existing policies within the company.

People involved in the breaches or potential breaches reported by the notifier shall be excluded from the investigation team and are also not allowed to participate in the assessment of the notification or the determination of the actions to be taken regarding the notification.

Conflicts of interest are reported to the board of directors if the management/ executive board is targeted in the notification. If the board of directors appears to be involved, the general meeting of the Company will be informed.

4-Feedback
The notification manager will provide appropriate feedback to the notifier within a reasonable time, and at most within three months from the date of the acknowledgement of receipt of the notification. This feedback shall include information for the notifier about the actions planned and/or taken and the reasons for these actions. He/she shall inform the notifier through the chosen internal notification channel.

5-Investigation report
Upon completion of the investigation, the investigation team will prepare a summary report, which will describe the investigation measures carried out. An edited, non-confidential and anonymized version of this overview report may be shared, on a need-to-know basis only, outside the investigation team with local or executive management to reach a final decision.

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

I. In case the (potential) breach is proven, relevant actions are identified with a view to countering the (possible) breach and protecting the Company; or

II. In case the investigation shows that there is insufficient or no evidence of the (possible) violation, no further action will be taken.

The notifier will be informed via his/her chosen internal notification channel about the closure of the notification and the decision taken.

4.3.1 The notification managers

The Company's notification managers are designated as:

- Bert Nijs, Corporate Counsel WEngage,
- Maud Kelders, Privacy Officer WEngage,
- Rosalie Faes, HR lawyer WEngage.
- Juan Alleman, Lawyer

Each notification manager performs his/her duties independently and without any conflict of interest. He/she is subject to a duty of confidentiality.

4.3.2 Records of notifications

The Company will maintain a record of all notifications received, in accordance to the confidentiality measures set out in article 5.1 of this policy.

These notifications and related information are kept for as long as the contractual relationship between the notifier and the Company is ongoing.

Where for the purpose of notification, with the consent of the notifier, a telephone line with call recording or another voice message system with call recording is used, the Company will record the oral notification as follows:

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

If a telephone line without call recording or other voice message system without call recording is used, the Company will record the verbal notification in the form of an accurate record of the conversation, prepared by the staff member responsible for handling the notification. The notifying party will be given the opportunity to check and correct this written record and sign for approval.

In the event of a face-to-face meeting with the notification manager, provided the notifier agrees, a complete and accurate record of the interview will be kept in a durable and retrievable form. The Company has the right to record conversation as follows:

- by a call recording in a durable and retrievable form;
- by an accurate record of the interview. The notifier will be given the opportunity to check this report, correct it and sign for approval.

4.4 External notification channels

1-
Notifiers may use an external notifying channel after notifying through the internal channels or directly through the external notification channels if they consider it more appropriate.

2-
The Federal Coordinator is charged by the Belgian legislator with coordinating notifications, entered through external channels. A RD is in the pipeline assigning the Federal Coordinator's task to the Federal Ombudsman.
The Federal Coordinator is responsible for receiving external notifications, checking their admissibility and forwarding them to the competent authority for investigation, which will be different depending on the subject of the notification.

This authority could 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 College of Supervision 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 protection of privacy and personal data), etc.

In exceptional cases, the Federal Coordinator may also conduct the investigation itself.

The Federal Coordinator's contact details are as follows (subject to the entry into force of the RD):
Address: Leuvenseweg 48 bus 6, 1000 Brussel
Online complaint: Filing a complaint | Federaalombudsman.be
E-mail: contact@federaalombudsman.be
Telefon: 0800 99 961
Fax: 02 289 27 28

5 Protective measures

The Company is committed making every effort to provide individuals covered by this policy with appropriate and effective protection to the extent that the disclosure complies with the terms of the Act in particular by taking the following measures:

5.1 Guarantee of confidentiality

The Company assures that it will take the necessary steps to ensure that employees and others can make a notification to the Company in confidence.

The Company commits itself to provide the necessary measures so the identity of the notifier cannot be disclosed without his/ her free and explicit consent to any person other than staff members who are authorized to receive or follow up notifications.

This also applies to all information from which the identity of the notifier can be directly or indirectly deduced.

Notwithstanding the previous paragraph, the identity of the notifier of the breach may be disclosed when it is under special legislation in the context of an investigation by the national authorities or in the context of a judicial proceedings is necessary and proportionate, in particular to protect the rights of defence of the data subject.

In the latter case, the notifier shall be informed of the disclosure of his or her identity before it takes place, unless such information would jeopardize ongoing investigations or judicial proceedings. This is the case, for example, if the notifier represents a key witness in court or in cases of unjustified or unlawful notification, to protect the rights of the person's defence.

5.2 Protection against reprisals

Any form of reprisals against the individuals referred to in article 2.1 who will be protected under this policy, including threats of retaliation and attempted retaliation, is prohibited, particularly in the following forms:

- suspension, temporary retirement, dismissal or similar action
- demotion or refusal of promotion
- change of job, change of workplace, reduction of pay, change of working hours;
- suspension or refusal of training
- negative performance appraisal or negative reference;
- imposition or application of a disciplinary measure, reprimand or other sanction, including a financial sanction;
- coercion, intimidation, harassment or exclusion;
- discrimination, adverse or unequal treatment;
- failure to convert a temporary employment contract into an indefinite employment contract, while the employee had the legitimate expectation that he/ she would be offered an employment contract for an indefinite term;
- non-renewal or early termination of a temporary employment contract;
- damage, including damage to reputation, particularly on social media, or financial loss, including loss of turnover and income;
- blacklisting on the basis of an informal or formal agreement for an entire sector or industry, preventing the notifier from finding employment in the sector or industry; early termination or cancellation of an agreement for the supply of goods or services
- revocation of a licence or permit;
- psychiatric or medical referrals.

6 Processing of personal data

For the purposes of the internal notification procedure, the Company is considered to be responsible for the processing of personal data.

Any processing of personal data for the purposes of this policy shall be carried out in accordance to applicable personal data protection legislation, including the European General Regulation Data Protection ("GDPR").

The following personal data may be processed in the context of a notifier: name, position, date of employment, contact details and e-mail address of the notifier and of people, involved in the breach,

any identified or identifiable information provided by the notifier and collected in the context of the internal investigation. This processing of data is done in the context of complying with a legal obligation and/or the legitimate interest of the company, to the extent that the internal notification channel transcends legal objectives, in particular, the detection of breaches, ensuring the security and ethical conduct of the Company.

Personal data that is clearly not relevant to the processing of a notification will not be collected or, if collected, deleted as soon as possible. Such data will be kept when the breach notified is time-barred and in any case for a period of five years after the notification was made.

The identity of the notifier may only be disclosed with the notifier's consent. Other data also remain strictly confidential and are shared only on a strict need-to-know basis.

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

For more information on the processing of personal data, please refer to the Privacy Statement for employees, job applicants, independent service providers and temporary workers and the Privacy Policy available on the Company's internal communication channels.

7 Effective date

This policy comes into force on 3 March 2023 for an indefinite period.

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