bpostgroup
Rethink the possible.

Compliance & Ethics

Speak Up Policy

Version: 2
Entry into force: 7 May 2025

Key message

This Speak Up Policy (the 'Policy') builds upon the first version published in 2023 and has been updated to incorporate the latest legislative requirements across all jurisdictions where bpostgroup operates. Its purpose is to ensure full compliance with current laws and regulations while reinforcing transparency and trust in the process of reporting and addressing concerns.

It provides individuals associated with bpostgroup – such as employees, trainees, suppliers, and suppliers (as defined below) – with clear guidelines and secure reporting mechanisms to raise concerns about potential legal violations or breaches of bpostgroup's Code of Conduct and other company policies, in full confidentiality and without fear of retaliation.

This Policy has been issued by bpostgroup in order to:

- ensure compliance with legal and regulatory obligations while upholding high ethical standards;
- provide secure reporting channels for raising concerns confidentially and without fear of retaliation;
- reinforce trust, integrity, and transparency across all levels of the organization.

By enabling everyone to speak up about their concerns, this Policy actively contributes to safeguarding integrity within bpostgroup and to fostering a healthy and respectful work environment for all.

Table of content

1.
What is this policy about?

At bpostgroup, we are committed to conducting our business with the highest standards of integrity, compliance, and ethics across all our business operations and activities. These principles are the cornerstone of a workplace culture built on trust, safety, and ethical responsibility – values we hold in the highest regard.

This Speak Up Policy plays a crucial role in fostering and strengthening this culture. It provides independent and impartial channels for reporting concerns about actual or potential legal violations or breaches of bpostgroup's Code of Conduct and/or other company policies, in a confidential and secure manner, without fear of retaliation. In particular, this Policy outlines the different reporting channels available within bpostgroup (including bpost S.A./N.V. and its subsidiaries) and explains how reports are managed.

Your reports help uncover and address issues that might otherwise go unnoticed. While we understand that raising such concerns can be challenging or intimidating, we encourage you to use our reporting channels and come forward to speak up. By doing so, you contribute to a healthier and more ethical work environment.

This Policy is applicable to each legal entity belonging to bpostgroup, except Radial USA and Landmark Global USA. If local legal requirements differ or impose stricter standards than those outlined in this Policy, these country-specific provisions are detailed in the country annexes in Section 15.

2.
Who can report a concern?

The following individuals can report a concern under this procedure:

- a bpostgroup employee;
- a bpostgroup volunteer or a trainee (paid or unpaid);
- a bpostgroup shareholder, member of the management or supervisory body of a bpostgroup entity, including non-executive directors;
- a person working for a bpostgroup (sub)contractor or supplier;

Former employees of bpostgroup as well as individuals who have applied for a position within bpostgroup may also use the reporting channels available under this procedure.

Please note that other individuals may be eligible to raise concerns depending on the country. For country-specific differences, consult the relevant country annex (see Section 15).

3.
What concerns can be reported?

You can report actual or potential legal violations which fall under the scope of the national whistleblowing rules (see Section 15), as well as actual or potential breaches of bpostgroup's Code of Conduct and other company policies.[1]

Examples of such misconduct include, but are not limited to:

- Abuse of company assets and resources
- Bribery
- Conflicts of interest
- Corruption
- Fraud
- Illegal taking of personal interests
- Illegal use of public funds
- Insider trading
- Inaccurate reporting or recordkeeping of financial and other data
- Misappropriation of funds, products, supplies, or equipment
- Misuse of personal data and violation of privacy
- Money laundering or violations of sanction laws
- Violation of competition laws
- Retaliation against someone who has reported a concern in good faith under this Policy

The aforementioned list is not exhaustive and is intended for illustrative purposes only. It may be possible to raise other types of concerns under local bpostgroup policies (see Section 15).

If you are a bpostgroup employee, you should continue to raise any grievances relating to your individual employment conditions and terms of employment through your usual HR channels.

If you doubt whether your concern falls under the scope of this Policy, we recommend you to first request further information from the Compliance department or the local entity reporting manager. This can be done through the Speak Up Tool.

[1] Throughout this Policy, the terms "concern(s)" or "misconduct(s)" refer to violations or potential violations that you become aware of and wish and are encouraged to report.

Do **not** use the reporting channels under this Policy:

- to report an immediate threat to life, health and safety or property. If emergency assistance is required, please contact local authorities or call the relevant country's emergency phone number;
- to report any information protected by national security, or covered by doctor/patient confidentiality or lawyer/client privilege, unless it concerns your personal medical data or exchanges with your lawyer. You should only report information obtained in a legal manner.

4. What are the conditions required to report a concern?

You must make your reports in good faith and should not rely on rumours, hearsay, or defamatory statements. Reporting in "good faith" means that you have **reasonable grounds to believe, at the time of reporting, that the facts reported are true.** If you raise a concern in good faith that later proves to be unfounded, you will not face any sanctions or negative consequences.

Your concerns must relate to actual or potential violations that have occurred or are very likely to occur **within bpostgroup and/or which relate directly to its activities,** and of which you have become aware within a professional context.

In summary, for bpostgroup to be able to handle a concern under this Policy, the following cumulative conditions must be met:

- you must be eligible to raise a concern under this Policy;
- you must have obtained such information within a professional context;
- you must have reasonable grounds to believe that the reported information is true;
- the subject matter of the concern must fall within the scope of this Policy;
- your report must be made via one of the channels described below.

5. Which channels are available to report a concern?

We encourage you to report concerns about actual or potential violations as soon as possible through bpostgroup's internal reporting channels.

You can report your concerns internally via the **Speak Up Tool**, the **telephone hotline** (see Section 5.1), or by sending a **registered letter** to the reporting manager of your local entity (please clearly indicate "CONFIDENTIAL" on the letter). Contact details of the relevant local entity reporting manager can be found in the country annexes (see Section 15).

In certain countries, it may also be possible to raise concerns via an **external authority** (see Section 5.2). In specific cases, **public disclosure** may also be an option under applicable legal conditions (see Section 5.3).

bpostgroup is only responsible for the internal reporting channels.

5.1 When can a concern be reported by using the internal channels?

If you are a bpostgroup employee, we encourage you to use bpostgroup's internal reporting channels as a complement to the usual communication channels. Therefore, if you believe that a (potential) misconduct covered by this Policy may have occurred, you are encouraged to first report it to your immediate superior, who may address it or escalate it as needed. However, if this is not possible or if his response is unsatisfactory, you can directly use the internal reporting channels.

If you are not a bpostgroup employee (e.g. former employee, external collaborator, etc.), you are also encouraged to report your concerns through these internal reporting channels, which are designed to provide a secure means for raising potential issues related to bpostgroup.

The following three internal reporting channels are available:

- the practical online Speak Up Tool: www.bpostgroup.com/ethics-and-behavior.
- the telephone hotline, with the applicable number for each country available via the following link: www.bpostgroup.com/ethics-and-behavior.
- the registered letter: the address of the relevant local entity reporting manager can be found in the country annexes (see Section 15).

The Speak Up Tool and telephone hotline are accessible at any time, 24 hours a day, 7 days a week. Reports made via the telephone hotline are transcribed and entered into the Speak Up Tool to ensure proper follow-up.

These internal reporting channels are designed to ensure **security and confidentiality**, protecting your identity as well as any third party mentioned in your report. Access is **strictly limited** to authorized members of the Compliance department of bpostgroup who are part of the Speak Up team, as well as the local entity reporting manager, provided the latter is handling your report and has been granted access to the Speak Up Tool or if your report was submitted via registered letter.

5.2 Is it possible to report a concern via an external authority channel?

It is recommended to first use one of the internal reporting channels: Speak Up Tool, telephone hotline, or registered letter to your local entity reporting manager. bpostgroup has set up the necessary procedures, teams and resources to investigate and address concerns reported through these channels. Therefore, using an internal reporting channel is an efficient and safe way of reporting your concern.

However, if your concern relates to the bpost S.A./N.V. or an EU subsidiary, you have the right to opt for reporting your concern externally to a competent authority. The rules for reporting your concern externally to a competent authority, the authority competent to receive it and the follow-up procedure vary from country to country. Please consult your country annex (see Section 15) for further information.

5.3 Is it possible to make a public disclosure instead of an internal or external reporting?

If you make a public disclosure, you make the concern you have identified accessible to the public. Examples of public disclosure include leaking information to the press, posting information online, publishing information in a book or magazine, etc.

For all EU countries, if you make such public disclosure, you will be protected against retaliation:

- if you have reasonable grounds to believe your concern presents an imminent or obvious threat to the public interest;
- if you consider that internal or external reporting has not resulted in adequate action;
- if you believe there is a significant risk of retaliation or that an investigation will not lead to a resolution.

If you make a public disclosure under circumstances not covered by the law, protection will not be granted.

For non-EU countries, consult the relevant country annex (see Section 15).

6. Is it possible to report a concern anonymously?

You may report a concern anonymously via the Speak Up Tool, the telephone hotline, or by registered letter to your local entity reporting manager, unless anonymous reporting is prohibited in your country (see Section 15).

Whether your report is anonymous or not, the Compliance department and your local entity reporting manager will protect your identity and guarantee full confidentiality. They are bound by a legal duty of confidentiality.

It is important that your report is precise and detailed, as checks will be made to determine the accuracy and seriousness of the reported facts. Anonymous reporting can limit the possibility to obtain additional clarifications and conduct a thorough follow-up, which is why we encourage you to identify yourself.

7. What information must be included in a report?

Your report must include clear, precise, and detailed information sufficient to enable an effective follow-up. **Specifically, your report should include at least the following elements:**

- your personal details (unless your report is anonymous);
- detailed description of your concern;
- background and chronological details of your concern;
- location(s), date(s), and timing, if known;
- details of any persons involved;
- supporting or documentary evidence, if available.

Providing as much details as possible will help facilitate handling concerns.

8. What happens after a concern is reported internally?

The process begins with identifying the appropriate entity responsible for handling your report, followed by a series of clearly defined steps to ensure an effective follow-up.

8.1 Who will be responsible for handling the reported concern?

Your concern raised via the **Speak Up Tool** or **telephone hotline** will be received by the Compliance department of bpostgroup (Speak Up team). The handling of your report will then be assigned based on the entity to which it relates, as follows:

- **If your report relates to bpost S.A./N.V. itself**, the follow-up, investigation, and feedback will be handled by the Speak Up team, which will act as the local reporting manager for bpost S.A./N.V.
- **If your report relates to another entity of bpostgroup**, the follow-up, investigation, and feedback will be handled by the competent person/body within the relevant subsidiary, who will act as local entity reporting manager for that subsidiary. In such case, the Speak Up team will transfer your report to the local entity reporting manager of that subsidiary for appropriate follow-up, investigation, and feedback.
- **If, due to its nature or extent, your report could be better handled by the Speak Up team**, it will be presumed that you agree to have them handle the investigation. In this case, the Speak Up team will act as your case handler and your report will not be forwarded to the local reporting manager of your entity. However, should you wish your report to be treated by your local entity reporting manager instead, please explicitly revoke your consent in the comment box of the report. It is recommended to not opt for this, as the Speak Up team will be best placed to investigate such concern.

You can also raise concerns by sending a **registered letter.** Depending on the address provided, your report will be handled by either the Speak Up team or by your local entity reporting manager.

Whether your report is handled by the Speak Up team or by your local entity reporting manager, the individual or team responsible will act as the **case handler** and will be responsible for communicating with you should further information be required and to provide you with feedback.

8.2 What are the different steps for handling a report?

Once the case handler has been designated, a structured process will be followed to ensure your report is handled effectively:

1. The case handler will acknowledge receipt of your report within 7 calendar days via the Speak Up Tool or by registered letter. A case number will be issued to follow up on your report. The acknowledgement of receipt does not mean that your report is deemed admissible.
2. The case handler will then assess whether your report falls within the scope of the applicable whistleblowing legislation (see Section 15), and you will then be informed whether your report is admissible. If your report is found inadmissible, it will be dismissed without further action being taken.
3. If your report is deemed admissible, the case handler will analyze the information reported and determine whether it is necessary to carry out an in-depth investigation. If that is the case, a thorough investigation will be carried out to fully uncover all relevant facts, including both incriminating and exonerating evidence. The investigation will be conducted in an independent, fair and unbiased manner with respect to all parties involved and in accordance with applicable laws and processes.

   Individuals involved in an investigation are expected to cooperate and answer all questions completely and honestly. Lying to the people performing the investigation as well as delaying, interfering with or refusing to cooperate with an investigation may lead to disciplinary measures. All parties involved, including the person who is the subject of your report, are entitled to confidentiality to avoid unnecessary damage to their reputation. Therefore, participation in or knowledge about an investigation requires maintaining strict confidentiality about the matter.
4. You will be informed of the investigation's progress within 3 months of the acknowledgement of receipt of your report:
   - If the investigation is completed, the findings will be compiled in a confidential final report, which will include observations and potential recommendations. This report will be sent to the management, which will determine whether to act on the recommendations provided.

     You will receive feedback on the outcome of the investigation. However, access to the confidential final report will not be granted. Other individuals involved in the investigation, including witnesses, will also be informed of the investigation's outcome in accordance with the principles of confidentiality. Also they will not be granted access to the confidential final report.
   - If further investigative measures are required after the first 3 months, you will be informed and receive further updates.
5. Once the final report has been sent and feedback provided, the case handler concludes its handling of your report.

9.
How is confidentiality protected?

The procedure for handling **all reports (anonymous and non-anonymous)** is designed to maintain **strict confidentiality.** This ensures that the identity of the individuals involved, as well as any details that could directly or indirectly reveal it, is protected and will not be disclosed without prior explicit consent. All documents related to your report are treated with the same level of confidentiality. Access to such information is strictly limited to individuals subject to a strict confidentiality obligation.

In particular, your identity or any information that could reveal it, will only be shared if required by law, for example in the context of investigations by national authorities or legal proceedings.

bpostgroup reserves the right not to process a concern if it relates to your personal situation and your refusal to allow disclosure of your identity makes it impossible to verify the reported information.

10.
How is protection against retaliation ensured?

If you report a concern in good faith in accordance with this Policy, you will be protected against retaliation related to your report.

In practice, this means you are protected from the following forms of retaliation (non-exhaustive list):

- disciplinary measures, such as suspension, disciplinary layoff, dismissal;
- demotion or refusal of promotion;
- training suspension;
- negative performance evaluation;
- coercion, intimidation, harassment, or ostracism;
- discrimination, disadvantageous or unfair treatment;
- non-renewal or termination of a commercial contract;
- harm, including damage to the person's reputation.

These **protective measures also extend to other categories of individuals**, i.e. facilitators who could assist you during the reporting process and whose help should remain confidential, and to third parties associated with you who may face retaliation in a work context, such as colleagues, family members, or the company you work for or have a professional relationship with.

If you believe to be subject to retaliation, we strongly encourage you to take immediate action by submitting a new report through the internal reporting channels. This ensures that your concern is promptly addressed and that you continue to receive the support and protection you deserve.

Any bpostgroup employee who engages in actions that may be considered retaliatory and/or as obstructing the handling of a concern or who encourages others to act in this manner may be subject to sanctions or legal proceedings, including disciplinary measures, dismissal and criminal prosecution.

11.
What are the rights of persons regarding whom a concern is reported?

When a concern is reported, the persons regarding whom the concern is reported will be informed of the nature of the allegations made against them and will be given the opportunity to provide information allowing the veracity of the reported facts to be verified.

These individuals will not be informed or will only be informed after precautionary measures have been taken, if there are reasonable grounds to believe that they are in a position to destroy data, manipulate files or otherwise endanger or compromise the investigation of your report.

12.
How is personal data processed?

In the context of this Policy, bpostgroup may collect and process personal data based on the obligations directly imposed on it by the EU Whistleblowing Directive (Directive (EU) 2019/1937) and national legislation. Therefore, bpostgroup and its subsidiaries will comply with the GDPR (General Data Protection Regulation), as stipulated in the employee privacy notice and in the privacy Policy applicable to your entity.

Personal data will only be processed by bpostgroup to the extent necessary to receive a report, examine its admissibility, verify the facts reported and to take any other necessary measures resulting from the outcome of the handling of such report, including guaranteeing the absence of retaliation.

bpostgroup may process the personal data provided by the reporting person, and any other personal data collected during the handling of a report including but not limited to:

- the reporting person's identity (surname and first names) and function (in case the report is not anonymous) and their family members where relevant ;

- the identity (surname and first names) and function of the person(s) mentioned in the report;
- the identity (surname and first names) and function of the person(s) receiving and handling the reported concern;
- the identity (surname and first names) and functions of person(s) providing information necessary to the handling of the report;
- the information contained in the report;
- the information collected during the handling of the report;
- the investigation report.

The legal basis for collecting and handling such personal data is bpostgroup's requirement to comply with its legal obligations resulting from EU Whistleblowing Directive (Directive (EU) 2019/1937), and where not strictly necessary by law its legitimate interests. The handling of special categories of personal data may be required with a view to establishing, exercising, and defending legal claims.

Each bpostgroup legal entity is the data controller of the personal data. During the reception and handling of the report, personal data may be received and/or handled and/or transferred to other bpostgroup entities, specifically bpost S.A./N.V. managing the Speak Up Tool. The transfer of personal data to countries outside the European Union which do not ensure a sufficient level of protection will be subject to appropriate guarantees.

Personal data will be kept in the secure Speak Up Tool. The persons who may have access to the personal data, collected during the handling of a report, include all persons appointed to handle and/or assist in handling reports and/or to take appropriate measures following such reports. This may include persons within the entities of bpostgroup or within third parties such as the provider of the Speak Up Tool and telephone hotline or law firms retained by entities of the bpostgroup to assist in handling reports. All such persons are bound by an obligation of strict confidentiality.

bpostgroup may also disclose personal data to the competent authorities, including judicial authorities, to comply with its legal obligations.

All personal data collected under this procedure shall be kept and deleted according to the applicable legislation in each country (see Section 15).

Any person whose personal data is collected and processed has the rights described below:

- a right to object to such processing. However, this right of opposition cannot be exercised to prevent bpostgroup from addressing reports;
- a right of access to his or her personal data, i.e. the right to know whether personal data is being processed and, if so, to access it with information on certain characteristics of the processing (in accordance with the legislation in force);
- the right to rectify inaccurate personal data and to complete incomplete personal data;
- the right to erasure of personal data, which allows the data subject to any applicable legal retention obligations to be erased in certain cases (e.g. personal data that are no longer required for an internal investigation and its follow-up);
- the right to limit the processing of personal data (including, in certain cases, to obtain the suspension of processing).

Depending on the circumstances and in order to ensure a compliant processing of personal data, some restrictions might apply.

These rights can be exercised by sending a request to the data controller via privacy@bpost.be.

Any person whose personal data are collected and processed in the context of handling a report has the right to lodge a complaint with the competent supervisory authority, in particular in the Member State in which he/she has his/her habitual residence or place of work, or in which he/she alleges that a breach of the regulations in force has occurred.

13.
Whom to contact with questions?

Any questions or comments about this Policy should be addressed to bpostgroup's Compliance department (Speak Up team). This can be done through the Speak Up Tool or via the following e-mail address: **speak-up@bpost.be**. This e-mail address cannot be used for submitting a report.

14.
How is this policy made accessible and kept up to date?

This Speak Up Policy:

- is an internal document, available to employees on bpost4me and communicated across all bpostgroup subsidiaries through appropriate internal channels;
- is also available externally on the bpostgroup website;
- is an evolutive document, subject to periodic review and updates to reflect legislative or regulatory changes, organizational needs, and best practices.

Updates will be communicated to all relevant individuals within bpostgroup, including employees, contractors, and other stakeholders as applicable.

Country annexes

Australia

1 Which violations can be reported?

In addition to the concerns mentioned in Section 3 of this policy, you can make a report under this policy if you have reasonable grounds to suspect the information you are reporting concerns misconduct or an improper state of affairs or circumstances in relation to bpostgroup.

Certain violations which may be reported include, but are not limited to:

1. breaches under the Corporations Act 2001 (Cth);
2. breaches under other financial sector laws enforced by either Australian Securities and Investment Commission ("ASIC") or the Australian Prudential Regulatory Authority ("APRA");
3. breaches under the Insurance Act 1973 (Cth) or the Life Insurance Act 1995 (Cth);
4. breaches under Superannuation Industry (Supervision) Act 1993 (Cth);
5. an offence against other laws of the Commonwealth and that is punishable by imprisonment for a period of 12 or more months; or
6. matters which represent a danger to the public or the financial system.

2 Who is the responsible local reporting manager, and how can they be contacted?

For FDM:
National Human Resource Manager, HR Department, FDM Warehousing Pty Ltd, P.O. Box 6566, Wetherill Park NSW 1851 - Australia, **hr@fdm.com.au**.

3 Where and how can I report externally?

You may report your concerns externally to:

- ASIC or APRA;
- a lawyer, if it is for the purpose of obtaining legal advice or legal representation in relation to the whistleblowing process and protections set out in this policy, and as otherwise regulated by Part 9.4AAA of the Corporations Act 2001 (Cth);
- a member of the State or Commonwealth Parliament or legislature of a Territory, or a journalist, but only for the purpose of making a "**public interest**" or "**emergency**" report or disclosure.

A "**public interest**" or "**emergency**" report or disclosure is defined as follows:

A "**public interest**" report is where:

- a report to ASIC or APRA has already been made and at least 90 days have passed since the report was made;
- you have reasonable grounds to believe that no action has been or is being taken and that making a further report would be in the public interest;
- prior to making the public interest report, you have given written notice to ASIC or APRA that includes sufficient information to identify the previous report and states that you intend to make a "public interest" disclosure; and
- the extent of information disclosed is no greater than is necessary to inform the recipient of the "public interest" disclosure of the violation.

An "emergency" disclosure is where:

- a report to ASIC or APRA has already been made;
- you have reasonable grounds to believe the report concerns a substantial and imminent danger to the health or safety of one or more persons or the natural environment;
- prior to making the emergency report, you have given written notice to ASIC or APRA that includes sufficient information to identify the previous report and states that you intend to make an "emergency" disclosure; and
- the extent of information disclosed is no greater than is necessary than to inform the recipient of the "emergency" disclosure of the substantial and imminent danger that is posed.

4 Can I publicly disclose a concern?

No. If a violation is disclosed publicly, you may not be afforded the protections provided for under the Corporations Act 2001 (Cth). Violations must be reported either internally or externally and subject to the above criteria.

5 How long will the personal data be kept?

The documents relating to the reporting can be kept for 10 years after the end of the investigation. However, all personal data in these documents, collected under this policy shall be deleted after the end of the investigation, except in the event of criminal proceedings, a legal action or a disciplinary action, in which case the data shall be kept until a final decision has been taken to end the dispute between the parties.

1 800 763 983

Country annexes

Belgium

1 Which violations can be reported?

The type of violation you can report depends on the sector (public or private) to which the concerned entity belongs:

Entity	bpost S.A./N.V.	Belgian subsidiaries of bpostgroup
Legislative framework	Law of December 8, 2022 on the protection of whistleblowers in the public sector	Law of November 28, 2022 on the protection of whistleblowers in the private sector
Material scope	**1.** All integrity violations, i.e. each act that undermines or threatens to undermine the general interest and which: **a.** may be in breach of the national or EU laws, orders, circulars, or bpostgroup's Code of Conduct and other company internal policies; and/or **b.** entails a risk to human life, safety or health, or to the environment; and/or **c.** demonstrates a serious breach of professional obligations or of the proper management of a federal public-sector organization. **2.** The act of knowingly instructing or advising someone to commit the aforementioned violations.	**1.** Violations of directly applicable EU or national rules relating to the following areas: • public procurement; • financial services, products and markets and prevention of money laundering and terrorist financing; • product safety and conformity; • transport safety; • environmental protection; • 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 networks and information systems; • combating tax fraud; • combating social fraud. **2.** Violations affecting the financial interests of the European Union; **3.** Violations relating to the European Union's internal market, in which the free movement of goods, persons, services and capital is guaranteed, including violations of the Union's rules on competition and state aid.

Country annexes

Belgium

Excluded areas	**Violations relating to discrimination, bullying, violence, or sexual harassment in the workplace cannot be reported through the Speak Up channels since they do not fall within the scope of this Policy.** Other procedures are already in place to provide you with a specific protection: • If you feel you are a victim or witness of bullying, violence or sexual harassment or any other psychosocial risk in the workplace, we invite you to contact the person in charge of well-being at work or the psychosocial prevention team directly; • If you feel you are a victim or witness of discrimination, we invite you to first contact the psychosocial prevention team. If inappropriate, you can file a complaint under the Belgian anti-discrimination laws with the Institute for the Equality of Women and Men or the Interfederal Center for Equal Opportunities (Unia) or the Flemish Human Rights Institute.

2 Who is the responsible local reporting manager, and how can they be contacted?

For bpost SA of public law: the Compliance department, Boulevard Anspach 1, mailbox 1, 1000 Brussels - Belgium.

For Belgian subsidiaries of bpostgroup:

- Speos: HR director, HR Department, Bollinckxstraat 24/32, 1070 Brussels – Belgium.
- AMP: CHRO, HR Department, Lenniksebaan 451, 1070 Brussels – Belgium.
- Radial EU: HR Department, Industrieweg 18, 2850 Boom – Belgium.
- Active Ants BE: HR Department, Zeelandhaven 6, 3433 PL Nieuwegein - The Netherlands.
- Dynagroup BE: Legal Officer, Daelderweg 20, 6361 HK Nuth - The Netherlands.
- Eurosprinters BE: Legal Officer, Daelderweg 20, 6361 HK Nuth - The Netherlands.
- Staci Belgium (Staci Boom 1): HR Department, Scheldeweg 1, 2850 Boom – Belgium.
- Staci Belgium (Sepia): HR Department, Doornpark 57, 9120 Beveren – Belgium.

Reports made via the Speak Up Tool or the telephone hotline will be transferred to the responsible local entity reporting manager.

3 Where and how can I report externally?

You can report concerns related to bpost S.A./N.V. (company of public law) externally to the Federal Ombudsman's Centre for Integrity through one of the following channels:

- By filling the online whistleblower reporting form, available on their website: **https://www.federaalombudsman.be/en;**
- By sending them an e-mail at **integrity@federalombudsman.be;**
- By calling them on **0800 999 61** or **+32 (0)2 289 27 27**.

Concerns related to the Belgian private sector subsidiaries can be reported to the competent public authorities designated in the Royal Decree of 22 January 2023. The list of these authorities can be accessed here: **NL** / **FR**.

4 Can I publicly disclose a concern?

Yes.

5 How long will the personal data be kept?

The documents relating to the reporting can be kept for 10 years after the end of the investigation. However, all personal data in these documents, collected under this policy shall be deleted after the end of the investigation, except in the event of criminal proceedings, a legal action or a disciplinary action, in which case the data shall be kept until a final decision has been taken to end the dispute between the parties.

Country annexes
Belgium

6 Local adaptations to the policy

Admissibility assessment of your report

Concerns related to bpost S.A./N.V. (company of public law) will be subject to a separate admissibility assessment. In order to be admissible, your report must include at least the following details:

- your name and contact details, unless you choose to report anonymously;
- the date of your report;
- the nature of your relationship with bpost S.A./N.V.;
- a description of your concern;
- the date or time period when the concern occurred, is currently occurring, or is highly likely to occur.

Additionally, you should provide all relevant information available to you that could help assess the reasonable presumption of an integrity breach.

You will be informed of the outcome of this admissibility assessment **within 15 working days** from the receipt of your report.

Please note that a report may be deemed inadmissible if:

- it does not meet the formal legal requirements, including the absence of mandatory details (such as name and/or contact details, unless reported anonymously, date of the report, nature of the relationship with bpost S.A./N.V., employer's name, description of the alleged integrity violation, and relevant timeframe);
- it does not fall within the scope of this policy (either materially or personally);
- it is not based on a reasonable presumption that an integrity violation has occurred, is occurring, or is highly likely to occur.

If your report is deemed inadmissible, you will receive a communication explaining the decision, along with any relevant recommendations, if applicable.
If your report is deemed admissible, you will receive feedback on the progress of the investigation **within three months** of submission, with updates provided every three months thereafter until the investigation is concluded.

Extra-judicial protection against retaliation

If you believe you are a victim of retaliation, you are strongly encouraged to submit a new report through the internal reporting channels outlined in this policy. Alternatively, you may also seek assistance from the Federal Ombudsman's Centre for Integrity, which is responsible for protecting whistleblowers against reprisals. For contact details, please refer to the information provided above (cf. external reporting).

Support for reporting persons

You have the option to seek support from the Federal Institute of Human Rights, which provides whistleblowers with information and assistance confidentially.

You can contact the Federal Institute of Human Rights through one of the following channels:

- **Phone: +32 (0)479 88 57 40.**
- **E-mail: kl-la@firm-ifdh.be** or **info@firm-ifdh.be.**

0800 999 61

Country annexes

Canada

1 Which violations can be reported?

You can report any conduct or situation contrary to bpostgroup's code of conduct and other company policies.

2 Who is the responsible local reporting manager?

For Apple Express:
Quality department, 5300 Satellite Drive, Mississauga, Ontario L4W 5J2- Canada.

3 Where and how can I report externally?

Different procedures will apply depending on the nature of the concern that you wish to report.

- If your concern pertains to the suspected violation of Canadian competition laws (e.g., deceptive marketing practices, price fixing, etc.), you may report your concern to the Competition Bureau of Canada.
- If your concern relates to a suspected violation of securities laws (e.g., insider trading, etc.), your concern should be reported to the local securities commission of the province or territory in which you are located.
- If your concern relates to a suspected violation of federal privacy laws, you may report your concern to the Privacy Commissioner of Canada.
- If your concern relates to a suspected violation of employment standards, including any occupational health and safety laws or laws in respect of workplace violence and harassment, you may file a complaint with Employment and Social Development Canada's Labour Program.

4 Can I publicly disclose a concern?

Yes.

5 How long will the personal data be kept?

Data shall be retained in accordance with applicable privacy legislation.

6 Local adaptations to the policy

If your report concerns violations of the competition act, the protection against retaliation is applicable to any person who reports concerns and who has reasonable grounds to believe that competition laws have been violated.

1 800 235 6302

Country annexes

China

1 Which violations can be reported?

You can report concerns, which include but are not limited to the following:

1. serious violations of laws and regulations ;
2. major risks and hazards;
3. actions which endanger national security;
4. any conduct or situation contrary to bpostgroup's code of conduct and other company policies.

2 Who is the responsible local reporting manager?

For Landmark Global Asia:
HR Department , bpost International Logistics Beijing Co Ltd. (Ch) - C-201 No 17 Cangjingguan Hutong, Dongcheng District, Beijing – China.

3 Where and how can I report externally?

For violations in the field of market supervision, you can report through the internet (https://www.12315.cn/), telephone (12315), fax, mailing address, on-site to Market Supervision and Management Departments at all levels.

For the behavior of endangering national security, you can report to the national security organs in the following ways:

- Call the report receiving phone 12339;
- Via the national security organs Internet reporting acceptance platform website, www.12339.gov.cn;
- Deliver a letter of reporting to the national security organs;
- Report in person to the national security organs;
- Report through other state organs on the employer.

For criminal offenses, you can report to the local public security organs.

4 Can I publicly disclose a concern?

Yes, but with restrictions. For employees, we request you to first report the concern internally, unless there is an imminent threat to life, health and safety, property or public interest, or you have reported your concern to bpostgroup internally but no appropriate follow-up measures were taken. Disclosing a concern in public should be based on reasonable facts and expressed in good faith and in a compliant and reasonable way. Please note that slanders or disclosure of personal privacy, personal information, confidential information or trade secrets may lead to disciplinary actions and civil or criminal liability.

5 How long will the personal data be kept?

The documents relating to the reporting can be kept for 30 years after the end of the investigation. However, all personal data in these documents, collected under this policy shall be deleted or anonymized after the end of the investigation, except in the event of a disciplinary action against an employee. The personal information in these documents will be kept throughout the employment and be deleted or anonymized one year after termination of the employment. Notwithstanding the above, in case of criminal proceedings or a legal action, the data shall be kept until a final decision has been taken to end the dispute between the parties.

400 120 3062

Country annexes

France

1 Which violations can be reported?

You can report concerns regarding the following:

1. Crimes, misdemeanours, threats or damage to public interests, including violations of French and international law;
2. Any conduct or situation contrary to bpostgroup's code of conduct and other company policies.

For more detailed information on the personal and material scope of application of the whistleblowing policy, please consult your company's whistleblowing policy.

2 Who is the responsible local reporting manager?

For IMX:
HR department, 1110 bis Avenue du Général Leclerc,
Bâtiment 18 – 1B, 93500 PANTIN – France.

For STACI: Service Juridique, BP 59124,
95074 CERGY-PONTOISE – CEDEX – France.

3 Where and how can I report externally?

The list of the 42 competent authorities and clear information on external reporting is available in the decree n°2022-1284 dated 3/10/2022. Each competent authority is due to publish information on its whistleblowing procedure.

4 How long will the personal data be kept?

Reports which do not qualify as whistleblowing reports must be destroyed or anonymized immediately. If no measures are taken following a report, all data must be anonymized or destroyed within 2 months from the closing of the investigation. In case measures are taken, data can be kept until such measures are implemented and during the applicable prescription period during which such measures may be challenged.

0805 080 339

Country annexes

Germany

1 Which violations can be reported?

You can report concerns regarding the following topics:

1. offences which are punishable by law,
2. violations which are subject to a fine, insofar as the violated provision serves to protect life, body or health or to protect the rights of employees or their representative bodies,
3. other violations of federal and state legislation as well as directly applicable legal acts of the European Union and the European Atomic Energy Community:
   - **a.** on combating money laundering and terrorist financing, including in particular the Money Laundering Act and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EU) No 1781/2006 (OJ L 141, 5.6.2015, p. 1), as amended by Regulation (EU) 2019/2175 (OJ L 334, 27.12.2019, p. 1). 1), as amended,
   - **b.** product safety and conformity requirements,
   - **c.** road safety requirements concerning road infrastructure safety management, safety requirements in road tunnels and admission to the occupation of road haulage operator or road passenger transport operator (bus and/or coach undertakings),
   - **d.** requirements to ensure the safety of railway operations,
   - **e.** maritime safety requirements concerning European Union rules for the recognition of ship inspection and survey organisations, carrier's liability and insurance in respect of the carriage of passengers by sea, approval of marine equipment, maritime safety inspection, seafarers' training, registration of persons on board maritime passenger ships and European Union rules and procedures for the safe loading and unloading of bulk carriers,
   - **f.** civil aviation safety requirements for the prevention of operational and technical safety hazards and for air traffic control;
   - **g.** requirements for the safe transport of dangerous goods by road, rail and inland waterway;
   - **h.** requirements for environmental protection;
   - **i.** requirements for radiation protection and nuclear safety;
   - **j.** requirements for the promotion of the use of energy from renewable sources and energy efficiency;
   - **k.** requirements for food and feed safety, organic production and labelling of organic products, on the protection of geographical indications for agricultural products and foodstuffs, including wine, aromatised wine products and spirit drinks and traditional specialities guaranteed, on the placing on the market and use of plant protection products and on animal health and welfare, as they relate to the protection of animals kept for farming purposes, the protection of animals at the time of killing, the keeping of wild animals in zoos, the protection of animals used for scientific purposes and the transport of animals and related operations,
   - **l.** on standards of quality and safety of organs and substances of human origin, medicinal products for human and veterinary use, medical devices and cross-border patient care,
   - **m.** on the manufacture, presentation and sale of tobacco and related products,
   - **n.** on the regulation of consumer rights and consumer protection in relation to contracts between traders and consumers and on the protection of consumers in the field of payment accounts and financial services, indication of prices and unfair commercial practices,
   - **o.** on the protection of privacy in the electronic communications sector, the protection of privacy in electronic communications, the protection of confidentiality of communications, the protection of personal data in the electronic communications sector, the protection of the privacy of users' terminal equipment and of information stored in such terminal equipment, the protection against unreasonable harassment by means of advertising by telephone calls, automatic calling machines, facsimile machines or electronic mail and by means of calling line identification and calling line identification and subscriber directory listing,
   - **p.** the protection of personal data within the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data in the electronic communications sector. April 2016 on the protection of individuals with regard to the processing of personal data,on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)

Country annexes
Germany

(OJ L 119, 4.5.2016, p. 1; L 314, 22.11.2016,p. 72; L 127, 23.5.2018, p. 2) in accordance with Article 2 thereof,

q. on security in information technology within the meaning of Section 2(2) of the BSI Actof digital service providers within the meaning of Section 2(12) of the BSI Act,

r. on the regulation of the rights of shareholders of public limited companies,

s. on the audit of financial statements of public interest entities in accordance with Section 316aSentence 2 of the German Commercial Code,

t. on accounting, including bookkeeping, of companies that are capital market-oriented within the meaning of Section 264d of the German Commercial Code, of credit institutions within the meaning of section 340 (1) of the Commercial Code, financial services institutions within the meaning of section 340 (4) sentence 1 of the Commercial Code,securities institutions within the meaning of section 340 (4a) sentence 1 of the Commercial Code,institutions within the meaning of section 340 (5) sentence 1 of the Commercial Code,insurance undertakings within the meaning of section 341 (1) of the Commercial Code and pension funds within the meaning of section 341 (4) sentence 1 of the Commercial Code,

4. infringements of federally and uniformly applicable regulations for contracting authorities concerning the procedure for the award of public contracts and concessions and concerning legal protection in these procedures from the time the relevant EU thresholds are reached,

5. infringements covered by section 4d(1) sentence 1 of the Financial Services Supervision Act (Finanzdienstleistungsaufsichtsgesetz), unless otherwise provided for in section 4(1) sentence 1,

6. infringements of legal provisions applicable to corporations and commercial partnerships,

7. infringements in the form of agreements aimed at improperly obtaining a tax advantage contrary to the object or purpose of the tax law applicable to corporations and commercial partnerships,

8. infringements of Articles 101 and 102 of the Treaty on the Functioning of the European Union as well as infringements of the legal provisions referred to in section 81(2) number 1, 2 letter a and number 5 as well as paragraph 3 of the Act against Restraints of Competition.

9. infringements of the provisions of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1);.

10. statements by civil servants that constitute a breach of the duty to comply with the Constitution;

11. breaches of the protection of the European Union's financial interests within the meaning of Article 325 of the Treaty on the Functioning of the European Union, and;

12. infringements of internal market rules within the meaning of Article 26(2) of the Treaty on the Functioning of the European Union, including European Union rules on competition and state aid that go beyond paragraph 1(8).

2 Who is the responsible local reporting manager, and how can they be contacted ?

For radial EU:
HR department, Industrieweg 18, 2850 Boom – Belgium.

For Active Ants DE:
HR Department, Zeelandhaven 6, 3433 PL Nieuwegein - The Netherlands.

3 Where and how can I report externally?

Germany shall set up an external reporting office at Bundesamt für Justiz, which can be reached via this **link.**

4 How long will the personal data be kept?

Recordings of telephone calls must be deleted as soon as they have been written down.
Other documentation of the report must be deleted two years after the case is closed.

0800 181 2396

Country annexes

Italy

1 Which violations can be reported?

You can report concerns regarding violations of national or European Union regulatory provisions that harm (i) the public interest or (ii) the integrity of the company (including violations of the code of conduct of bpostgroup).

2 Can I report my concern anonymously?

Anonymous concerns are not expressly permitted under Italian law.

However, the protection for whistleblowers is extended also to anonymous ones only where their identity has been discovered and they have suffered retaliation because of it.

3 Who is the responsible local reporting manager, and how can they be contacted?

For radial EU:
HR department, Industrieweg 18, 2850 Boom - Belgium.

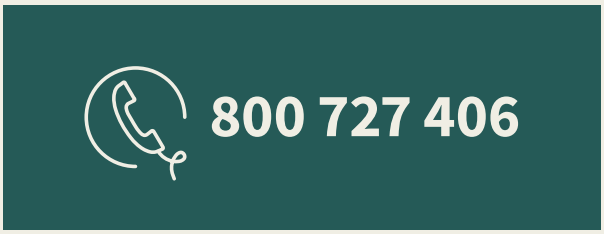
4 Where and how can I report externally?

Via the National Anti-Corruption Authority (ANAC, **www.anticorruzione.it**), by the following means:

- in writing via the IT platform;
- via telephone lines or voice messaging systems;
- at the request of the reporting person, by means of a face-to-face meeting set within a reasonable time.

5 How long will the personal data be kept?

The personal data are kept for as long as necessary to process the concern and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure.



Country annexes

Netherlands

1 Which violations can be reported?

In addition to the concerns that are stipulated in section 3 of this policy, you can report a concern in case of a (suspicion of a) wrongdoing (in Dutch: “misstand”). A wrongdoing is defined as:

1. A breach or danger of a breach of Union law, being an act or failure to act that is:
   a. Unlawful and relates to the Union acts and areas falling within the material scope referred to in Article 2 of the Directive (EU) 2019/1937; or
   b. Defeats the object or the purpose of the rules in the Union acts and areas falling within the material scope referred to in Article 2 of the Directive (EU) 2019/1937.
2. An act or failure to act on the following, where the general public interest is at risk:
   a. A breach or danger or breach of (i) a statutory provision or (ii) internal rules and procedures of bpost which entail a specific obligation that is based on legal requirements; or
   b. A danger for the public health, the safety of people, the environment or the proper functioning of a public service or company as a consequence of an improper act or failure to act.
   c. The general public is considered to be at risk in any case if (i) the act or failure to act not only affects personal interests, and (ii) there is a pattern or structural character to it or the act or failure to act is severe or extensive

2 Who is the responsible local reporting manager, and how can they be contacted?

For Dynagroup:
Legal Officer, Daelderweg 20, 6361 HK Nuth - The Netherlands.

For Radial EU:
HR Department, Industrieweg 18, 2850 Boom – Belgium.

For Active Ants NL:
HR Department, Zeelandhaven 6, 3433 PL Nieuwegein - The Netherlands.

3 Where and how can I report externally?

You can report to the Whistleblowers Authority (in Dutch: “Huis voor Klokkenluiders”) or any of the other competent authorities as mentioned in section 2c of the Whistle blower Protection Act (in Dutch: “Wet bescherming klokkenluiders”). Competent authorities are for example the Netherlands Authority for Consumers & Markets and the Dutch Data Protection Authority.

4 How long will the personal data be kept?

All personal data in these documents, collected under this policy shall be deleted after the end of the investigation, except in the event of criminal proceedings, a legal action or a disciplinary action, in which case the data shall be kept until a final decision has been taken to end the dispute between the parties.

5 Local adaptations to the policy

In addition to making a report through the Speak Up Tool, telephone hotline or by registered letter to your local entity reporting manager (Section 5), you can request an in-person meeting within a reasonable time to report your concern.

An employee is also allowed to contact an advisor on the suspicion of a wrongdoing. This person can for example be a (internal or external) confidential advisor (in Dutch: “vertrouwenspersoon”).

In Netherlands, you can also make a public disclosure (see section 5.3) if you reported your concern externally to the competent authority (after an internal report or not), but you have reasonable reasons to believe that appropriate follow-up measures were not taken within the legal timeframe.

0800 022 0441

Country annexes

Poland

1 Which violations can be reported?

An unlawful or fraudulent act or omission relating to:

1. corruption;
2. public procurement;
3. financial services, products and markets;
4. counteracting money laundering and terrorism financing;
5. product safety and compliance with requirements;
6. transport safety;
7. environmental protection;
8. radiological protection and nuclear safety;
9. food and feed safety;
10. animal health and welfare;
11. public health;
12. consumer protection;
13. protection of privacy and personal data;
14. security of networks and IT systems;
15. financial interests of the State Treasury of the Republic of Poland, local government units and the European Union;
16. the internal market of the European Union, including public law rules on competition and state aid as well as corporate taxation;
17. constitutional freedoms and rights of humans and citizens - occurring in an individual's relations with public authorities and not related to the areas indicated in points 1-16.

You can also report any conduct or situation contrary to bpostgroup's code of conduct and other company policies.

2 Who is the responsible local reporting manager, and how can they be contacted?

For Radial EU:
HR Department, Industrieweg 18, 2850 Boom – Belgium.

3 Where and how can I report externally?

You may report your concern externally to the Ombudsman (pol: Rzecznik Praw Obywatelskich) or the public authority competent to take follow-up measures in the legal areas indicated in point 1. The list of such authorities includes law enforcement authorities, including territorially competent police units and prosecutor's offices, the Supreme Chamber of Control, the President of the Office of Competition and Consumer Protection, the President of the Personal Data Protection Office, relevant labor inspection units, the Financial Supervision Authority, the Office of Electronic Communications, the European Anti-Fraud Office, the European Court of Auditors, the European Public Prosecutor's Office. Prior reporting through internal procedures is not required. External reports may be filed in writing or orally, as regulated under relevant procedures made available by each public authority. External channels will be available from December 25, 2024 at the latest.

4 How long will the personal data be kept?

Personal data are stored for a period of 3 years after the end of the calendar year in which follow-up measures were completed or after the completion of proceedings initiated by these activities; in the event that the report was refused, personal data are retained for a period of 3 years after the end of the calendar year in which the report was refused, unless documents related to the report constitute part of the files of preparatory proceedings or court or administrative court cases. In such a case, personal data will be stored until the final conclusion of the relevant proceedings. This does not apply to personal data collected in working documents created solely for the purpose of streamlining the proceedings, which are kept until the end of the investigation procedure.

5 Can I report anonymously?

Anonymous reports are accepted under the terms set out in this procedure.

800 005 266

* This procedure has been consulted with the employees' representative office in Poland.

** This procedure constitutes a group procedure within the meaning of Art. 28 section 8 of the Act of June 14, 2024 on the protection of whistleblowers (Journal of Laws 2024.928) established by companies belonging to one capital group within the meaning of Art. 4 point 14 of the Act of February 16, 2007 on competition and consumer protection (Journal of Laws of 2024, item 594). The companies within the group are as follows: Active Ants, Aldipress, AMP, Apple Express, bpost S.A./N.V., DynaGroup, Euro-sprinters, FDM, Freight 4U, IMX, Landmark Global, Leen Menken, Radial, Speos, Staci.

Country annexes

Singapore

1 Which violations can be reported?

You can report any conduct or situation contrary to bpostgroup's code of conduct and other company policies.

2 Who is the responsible local reporting manager, and how can they be contacted?

Landmark Global Asia:
HR Department , bpost International Logistics Beijing Co Ltd. (Ch) - C-201 No 17 Cangjingguan Hutong, Dongcheng District, Beijing – China.

3 Where and how can I report externally?

There is no specific overall external agency to report any violations to. However, there are certain external agencies to report certain matters to, by example:

1. In respect of the commission of or the intention of any other person to commit any arrestable offence punishable in accordance with section 424 of the Criminal Procedure Code 2010 of Singapore, please report to the officer in charge of the nearest police station or to a police officer.
2. In respect of employment-related matters such as employment violations, please report to the Ministry of Manpower of Singapore.
3. In respect of workplace harassment, please report to the Tripartite Alliance for Fair & Progressive Employment Practices.

4 Can I publicly disclose a concern?

Yes. However, the disclosure should not include any personal data which you do not have permission to disclose.

5 How long will the personal data be kept?

There is no prescribed duration for how long personal data can be kept for. However, the personal data must not be kept any longer than is necessary for the purpose for which the data is required (i.e. the investigation of the report).

800 852 3912

Country annexes

Spain

1 Which violations can be reported?

You can report any act or omission which may constitute an infringement of European Union law provided that:

1. fall within the scope of the acts of the European Union listed in Annex of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of on the protection of persons reporting breaches of Union law.
2. affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union Article 325 of the Treaty on the Functioning of the European Union (TFEU); or
3. have an impact on the internal market, as referred to in Article 26(2) TFEU, including infringements of European Union competition rules and aid granted by States, as well as infringements of the granted by States, as well as infringements relating to the internal market in relation to acts in breach of the rules of the infringements of the rules on corporation tax or practices intended to confer a tax advantage which distorts the tax advantage which would defeat the object or purpose of the legislation applicable to corporation tax.

You can also report omissions which may constitute a serious or very serious criminal or administrative offence. In any event, this shall be understood to include all criminal actions and very serious administrative offences involving financial loss to the Treasury.

Finally, you may report infringements of labour law in matters of health and safety at work, with special regards to harassment in all its variants: mobbing or psychological harassment, discriminatory harassment, sexual harassment and harassment towards the LGTBI collective.

2 Who is the responsible local reporting manager?

For Radial EU:
HR Department, Industrieweg 18, 2850 Boom – Belgium.

3 Where and how can I report externally?

You may report to the Independent Authority for Whistleblower Protection.

The information may be provided in writing, by post or by any electronic means provided for this purpose to the external information channel of the Independent Whistleblower Protection Authority, or verbally, by telephone or by voice messaging system.

At the whistleblower's request, it may also be submitted by means of a face-to-face meeting, within a maximum period of seven days. In cases of verbal reporting, the reporter shall be warned that the report will be recorded. informant that the communication shall be recorded.

4 How long will the personal data be kept?

The data processed may be kept in the information system for as long as is necessary to decide whether an investigation should be initiated into the facts reported and for the duration of the investigation. If the If In any event, for a maximum period of 10 years.

If it is established that the information provided or part of it is not truthful, it must be deleted immediately as soon as this circumstance comes to light.

In any case, after three months have elapsed from the receipt of the communication without any investigation having been initiated, the information must be deleted, unless the purpose of the conservation is to leave evidence of the operation of the system.

5 Local adaptations to the policy

At your request, a report can also happen during a face-to-face meeting, which will take place within a maximum of seven days. Likewise, you will be informed that the communication will be recorded and that your data will be processed.

900 905 460

Country annexes

United Kingdom

1 Which violations can be reported?

You can report any violations which amount to a “qualifying disclosure”. “Qualifying disclosures” must relate to one of the following “relevant failures”:

1. A criminal offence.
2. A breach of a legal obligation.
3. A miscarriage of justice.
4. A danger to any individual’s health or safety.
5. Damage to the environment.
6. Deliberate covering up of information relating to any of the above.

2 Who is the responsible local reporting manager?

For Landmark global:
HR Manager UK, HR department, Unit 3 Heathrow Logistics Park, Bedfont Road, Feltham, TW14 8EE - United Kingdom.

For Radial EU:
HR Department, Industrieweg 18, 2850 Boom - Belgium.

For Active Ants UK:
HR Department, Zeelandhaven 6, 3433 PL Nieuwegein - The Netherlands.

3 Where and how can I report externally?

You can make an external qualifying disclosure to a "prescribed" person in certain circumstances. “Prescribed” persons are mainly regulatory and professional bodies but includes other persons and bodies such as MPs. The relevant prescribed person will depend on the subject matter of the disclosure. A list of prescribed persons/ bodies and the relevant contact details can be found on the Government website: Whistleblowing: list of prescribed people and bodies - GOV.UK (www.gov.uk)

4 Can I publicly disclose a concern?

It is possible to make a “wider disclosure” to a person or body who is not a “prescribed” person, (without losing your protection under whistleblowing legislation), however, there are rigorous conditions which must be met to ensure protection for wider qualifying disclosures. These include:

1. **Belief**: You must reasonably believe that the information you disclose and any allegation contained in it are substantially true;
2. **Not for gain**: you cannot be acting for personal gain; and

You must:

1. Already have reported the same information to your employer or a prescribed person; **OR**
2. easonably believe (at the time of making the disclosure) that your employer will subject you to “detriment” or conceal or destroy evidence if you report it to them directly.

Your choice to make the disclosure must be reasonable in all the circumstances. For example: disclosure of a serious criminal offence to the police is more likely to be protected than if you made the disclosure to the media.

5 How long will the personal data be kept?

The data must not be kept any longer than is necessary for the purpose for which the data is processed (the investigation of the report).

(0) 808 189 1053

Country annexes

United States

1 Which violations can be reported?

All violations set forth in Section 3 of this Policy as well as any other reasonable, good faith belief of a suspected violation of any applicable law, rule or regulation.

2 Who is the responsible local reporting manager, and how can they be contacted?

For STACI: Service Juridique, BP 59124, 95074 CERGY-PONTOISE – CEDEX – France.

3 Can I report my concern anonymously?

Yes.

4 Where and how can I report externally?

Contact information for external reporting depends on the subject of the concern being reported. bpostgroup is committed to operating in compliance with its legal obligations. bpostgroup has established this policy and the procedures detailed herein to ensure that issues are raised to the company in a timely manner so they can be addressed and corrected promptly, as necessary. However, nothing in this policy or any other Company policy or materials prohibits, prevents, or otherwise limits employees from (1) reporting possible violations of federal or other law or regulations to any governmental agency, regulatory body, or law enforcement authority (e.g., EEOC, NLRB, SEC, DOJ, CFTC, U.S. Congress, or an Inspector General), (2) filing a charge or complaint with any such governmental agency, or (3) participating, testifying, or assisting in any investigation, hearing, or other proceeding brought by, in conjunction with, or otherwise under the authority of any such governmental agency. Employees are also not required to notify or obtain permission from the Company when filing a governmental whistleblower charge or complaint or engaging or participating in protected whistleblower activity.

5 Can I publicly disclose a concern?

We encourage you to report through the mechanisms set forth in this policy or to appropriate governmental authorities. Disclosures to the public are not necessarily legally protected in the United States and may, in some cases, violate other obligations you owe to bpostgroup.

Any employee who has a concern should use this policy and the procedures detailed herein to ensure that issues are raised to the company in a timely manner so they can be addressed and corrected promptly, as necessary.

6 How long will the personal data be kept?

Typically, seven years except in the event of civil or criminal proceedings, in which case the data shall be kept until such time as it is no longer needed or if a longer period of retention is required.

7 Local adaptations to the policy

bpostgroup encourages all employees to raise any concerns they may have to their supervisor or other member of management with whom they feel comfortable. It is the responsibility of anyone receiving a report under this policy to direct the report to the local reporting manager or the Compliance department for proper handling.

In conducting its investigation, the company will maintain the confidentiality of the reporting individual to the greatest extent possible. No employee will be subject to retaliation for making good faith reports under this policy. Additionally, those participating in an investigation may be asked to maintain the confidentiality of the investigation under certain circumstances in order to protect the integrity of the investigation. bpostgroup considers retaliation a violation of the company's policies and code of conduct. Anyone found to have retaliated against an individual for having made a report under this policy will be subject to discipline, up to and including termination of employment.

800 461 9330