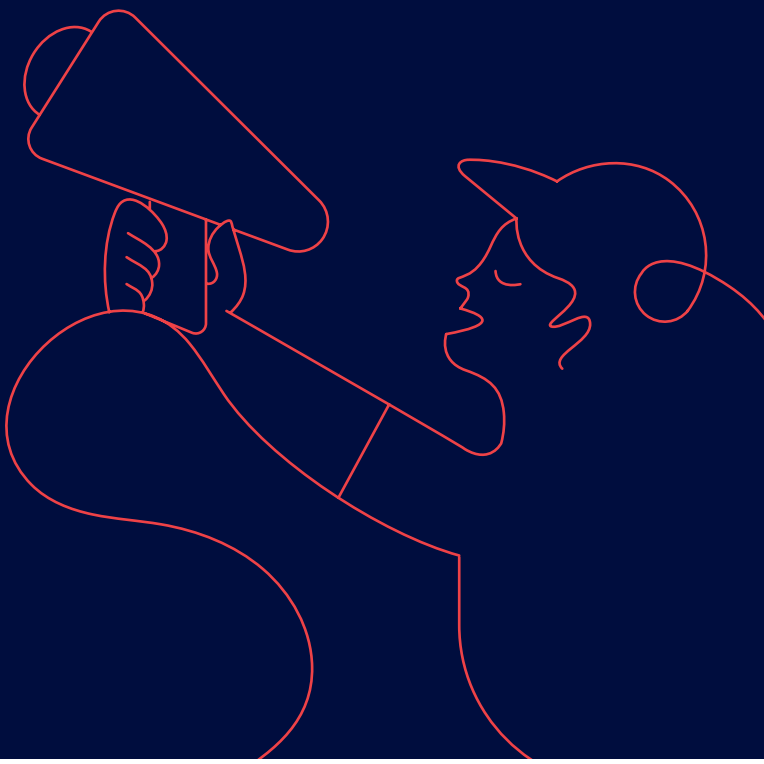
bpostgroup
You make us move.



Speak up Policy

1. What is this policy about?

bpostgroup considers integrity and compliance with laws and regulations as well as the code of conduct and other company policies to be extremely important. Integrity and compliance are essential to preserve bpostgroup's reputation, credibility, and trust of employees, clients, the public and other stakeholders, as well as to limit possible financial exposure.

This policy describes the reporting channels available at bpostgroup (bpost and its subsidiaries, except in the USA where specific reporting channels apply) where you can report in confidence and without fear of retaliation a situation you become aware of, which violates or seems to violate laws, regulations, the code of conduct or other company policies. Hereafter throughout this policy we use the term "concern" to refer to such misconduct or potential misconduct that you become aware of and wish and are encouraged to report.

It is not easy to raise such concerns. But it is important, and we encourage you to come forward and speak up. This policy will guide you in using the reporting channels. As an international group, bpostgroup must comply with various national rules. When differences between national rules are important (e.g. whether anonymous reporting is allowed), the policy refers to the country annex (see section 11).

2. Who can report a concern?

You may be an employee, a former employee, an external collaborator, or a person working for a subcontractor or supplier of bpostgroup.

To receive protection (see section 8), when reporting a concern, you must:

- have sufficient reasons to believe that the concern you are reporting is based on true and verifiable facts;
- follow the reporting procedure (see section 4) through (i) internal reporting, via the Speak Up Tool, telephone hotline or registered letter to your local entity reporting manager, (ii) reporting externally to the competent authority, or (iii) public disclosure.

3. What concerns can you report?

You can report violations or potential violations of laws and regulations which fall under the scope of the national whistleblowing rules (see your country annex), as well as violations or potential violations of bpostgroup's code of conduct and other company policies.

Examples of such misconduct:

- Fraud
- Bribery
- Violation of competition laws
- Money laundering or violations of sanction laws
- Conflicts of interest
- Insider trading
- Misuse of personal data and violation of privacy
- Abuse of company assets and resources
- Misappropriation of funds, products, supplies or equipment
- Inaccurate reporting or recordkeeping of financial and other data
- Bullying, workplace violence, or sexual harassment: if you feel victim or witness of bullying, workplace violence or sexual harassment or any other psychosocial risk at work, you are welcome to use the internal reporting channels under this policy, in which case your concern will be communicated to the team dedicated to psychosocial risks for treatment under the procedures specific to such matters. You can also contact them directly, in which case the procedures specific to such matters will also be followed
- Discrimination
- Violation of any company policies
- Retaliation against someone who has reported a concern in good faith under this policy

Your reported concern must directly relate to bpostgroup and its activities.

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 reporting manager (see section 5). This can be done through the “Ask a question” option in the Speak Up Tool.

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 your local authorities, or call your country’s emergency phone number;
- for grievances you may have regarding your terms of employment;
- to deal with personal or legal disputes unrelated to concerns of (potential) misconduct falling under the scope of this policy;
- to make accusations which you know are false. Doing so may lead to disciplinary measures if you are an employee. It may also lead to civil and criminal liability.

4. Which channels can you use to report a concern?

You can choose between:

- bpostgroup’s internal reporting channels, via the Speak Up Tool (see section 4.1), telephone hotline or registered letter to your local entity reporting manager;
- external reporting to the competent authorities, as mentioned in the country annex.

bpostgroup is only responsible for the internal reporting channels.

4.1 When can you report a concern by using the internal channels? Where can you find them?

If you are an employee, the internal reporting channels complement the usual channels of communication that bpostgroup encourages to use. Therefore, if you believe that (potential) misconduct covered by this policy may have occurred, you are encouraged to first report this to your immediate superior. The immediate superior can solve the issue himself, take the issue up with his own superiors or, if it is not possible or appropriate, report it through the Speak Up Tool, telephone hotline or registered letter to your local entity reporting manager.

If you feel for any reason that you cannot address your line manager or that the response provided by them could not be considered satisfactory, you can use the internal reporting channels via the Speak Up Tool, telephone hotline or registered letter to your local entity reporting manager.

If you are a former employee, an external collaborator or person working for a subcontractor or supplier of bpostgroup wishing to report, you can also use the internal reporting channels.

bpostgroup uses a practical online tool called Speak Up which you can use to report a concern and where you can follow-up the feedback which will be given to you. You can find the tool here:
www.bpostgroup.com/ethics-and-behavior

Besides, bpostgroup also offers a telephone hotline for reporting concerns verbally. This hotline can be reached on the number mentioned in your country annex (see section 11).

If you find it inappropriate to report your concern through the Speak Up Tool or telephone hotline managed by bpostgroup, you may report your concern directly to your local entity reporting manager by registered letter. You can find your local entity reporting manager’s address in your country annex (see section 11).

4.2 When can you report a concern by using an external authority channel? Where can you find it?

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 company 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 11).

4.3 Instead of reporting your concern internally or externally to the competent authority, can you make your concern public?

With a public disclosure, you make the concern that you have identified accessible for the public. Examples of public disclosure are 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 (see section 8) in two cases:

First case: If you reported your concern externally to the competent authority (after an internal report or not), but appropriate follow-up measures were not taken within the legal timeframe. When assessing whether appropriate follow-up measures were taken or not, you must be objective. Your assessment cannot depend on your subjective feelings.

Second case: If you have reasonable reasons to believe that:

- your concern may pose an imminent or manifest danger to the public interest, such as where there is an emergency or a risk of irreversible damage; or
- if you would report your concern externally to the competent authority, there is a real risk of retaliation against you or there is a low prospect of your concern being effectively addressed. This can by example be the case when evidence relating to your concern may be concealed or destroyed or when the external reporting authority may be in collusion with the perpetrator of the (potential) misconduct, or involved in the (potential) misconduct that is the subject matter of your concern.

For non-EU countries, please consult the country annex.

5. What happens after you have reported a concern?

Your concern reported via the Speak Up Tool or telephone hotline, will be received by the Compliance department of bpostgroup. The Compliance department will acknowledge receipt of your reported concern within 7 days via the Speak Up Tool.

If your reported concern relates to bpost S.A. / N.V. itself and bpostgroup, the follow-up, investigation and feedback will be entrusted to its Compliance department who will act as the local reporting manager for bpost S.A./N.V. and bpostgroup.

If your reported concern relates to a subsidiary of bpostgroup, the follow-up, investigation and feedback will be entrusted to the competent person/body within the relevant subsidiary who will act as local reporting manager for that subsidiary. In such case, the Compliance department will transfer your reported concern to the local reporting manager of that subsidiary for its follow-up, investigation and feedback. You can find your local entity reporting manager in your country annex (see section 11).

If, due to its nature or extent, your concern could be better handled at the level of bpostgroup, we assume that you consent to the investigation of your concern by the Compliance Department of bpostgroup who will act as a local reporting manager instead of the local reporting manager of your entity. In this case your report will be followed up by the Compliance Department of bpostgroup and will not be forwarded to the local reporting manager of your entity. However, should you wish your concern 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 Compliance Department of bpostgroup will be best placed to investigate such concern.

If you report your concern by registered letter to your local entity reporting manager, your local entity reporting manager will manage your concern directly. He will acknowledge receipt of your reported concern within 7 days, unless your report is anonymous.

The Compliance department or local entity reporting manager can take the following decisions regarding your reported concern:

- the report is inadmissible if the concern does not fall under the scope of application of this policy;
- the follow-up is stopped when the concern is unfounded or does not include sufficient evidence of verifiable facts for further investigation, or when the same concern has already been reported and investigated;

- further investigation of your reported concern is required to verify it;
- propose actions to management if the reported concern is sufficiently evidenced to finalize the investigation.

The Compliance department or local entity reporting manager will inform you of either one of these decisions within 3 months from the acknowledgement of receipt of your reported concern. Such follow-up is not possible if the report was made anonymously by registered letter to your local entity reporting manager.

When possible, the Compliance department or your local entity reporting manager will also inform you via the Speak Up Tool of the result of the investigation if this was not already included in the initial follow-up (after 3 months).

Your reported concern will be investigated in an independent, fair and unbiased manner with respect to all parties involved and in accordance with relevant laws and principles (including fair process). Details of the concern, your identity and the identity of anyone else mentioned in your report, are kept confidential throughout and after the investigation and are only shared on a need-to-know basis.

If you become involved in an investigation, you need 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 concern, are entitled to confidentiality to avoid unnecessary damage to their reputation. Therefore, if you participate in or learn about an investigation, you must keep the matter confidential.

6.
What are the rights of the person regarding whom you have reported a concern?

When a report is sent to the Compliance department or your local entity reporting manager, every person who is the subject of a concern that you have reported will be informed in writing by the local reporting manager of your reported concern about him . Such person may contact the Compliance department or your local entity reporting manager to exercise his right to access the file under the applicable data protection legislation. However, restrictions will apply:

- this person will only be informed of the (potential) facts that you reported which relates to him;
- this person will not be informed of your identity;
- the rights of this person are limited to the data relating to him.

The person mentioned in your report will be informed as soon as possible after receipt of your reported concern. Informing this person will not take place or will be delayed until precautionary measures have been taken, if there are reasonable grounds to believe that this person is in a position to destroy data, manipulate files or otherwise endanger or compromise the investigation of your reported concern.

Manifestly abusive data requests by the person who is subject of a concern can also be denied, e.g., repetitive requests of access to data.

7.
Can you report a concern anonymously? How is confidentiality protected?

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 country annex in section 11).

If you wish to identify yourself, the Compliance department and local reporting manager will protect your identity and thus guarantee confidentiality. They are bound by a duty of confidentiality which is a legal obligation.

It is important to note that checks will be made to determine the veracity and seriousness of the facts that you report as the basis of your concern. For this purpose, the reported facts must be sufficiently precise. Contacts with a non-anonymous reporting person may sometimes help to ascertain the reported facts at the basis a concern.

8.
Will you be protected against retaliation when reporting a concern?

If, while complying with this policy, you report in good faith a concern through (i) internal reporting (via the Speak Up Tool, telephone hotline or by registered letter to your local entity reporting manager), (ii) reporting externally to an authority, or (iii) public disclosure, bpostgroup will not retaliate against you, for instance disciplinary measures, change of working conditions, dismissal etc.

The terms “good faith” do not mean that you must be right in your assessment of the facts that your reported and gave

rise to your concern of (potential) misconduct. It means that you must provide all information in your possession and have reasonable grounds to believe, at the time of reporting, that the facts that your report as the basis of your concern of (potential) misconduct are true and verifiable and within the scope of this policy.

Any bpostgroup employee who engages in actions that may be considered retaliatory or who encourages other employees to retaliate against you when you have reported a concern in good faith may be subject to sanctions or legal proceedings, including disciplinary measures, dismissal and criminal prosecution.

The protection against retaliation does not apply to anyone who deliberately or recklessly make statements or disclosures in bad faith, e.g., motivated by a desire to harm and/or alleging questionable practices without any objective basis and facts underlying the alleged concern of (potential) misconduct.

9.
Are 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 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 the Compliance department or the local reporting manager to the extent necessary to investigate a reported concern and make decisions about it. bpostgroup may process the following personal data (not exhaustive):

- the identity (surname and first names) and function of the person reporting a concern (in case the report is not anonymous);
- 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 processing the reported concern;
- the reported facts leading to the concern;
- the answers to the questions and the various exchanges;
- the evidence collected during the investigation;
- the investigation report.

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

The Speak Up Tool, telephone hotline and receipt of your registered letter by your local entity reporting manager are set up and managed in a secure manner. They guarantee the confidentiality of the identity of those who report concerns and of those involved in the reported concerns. They prevent access by unauthorized employees and persons.

Whom can you contact with questions?

If you have any questions or comments about this policy, we invite you to contact the bpostgroup Compliance department: **speak-up@bpost.be**.

If your question relates to a subsidiary of bpost, please find the contact information of the local reporting manager in your country annex.

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?

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?

1. All integrity violations: each act that threatens or violates the public interest and which:

   a. does not comply with the code of conduct, or which may be in breach of the national or EU rules; and/or
   b. entails a risk to life, safety, health, the environment; and/or
   c. entails a serious breach of professional duty or good management of your entity.

2. Any conduct or situation contrary to bpostgroup's code of conduct and other company policies.

2 Who is the responsible local reporting manager?

For bpost SA de droit public:

the Compliance department, Boulevard Anspach 1, mailbox 1, 1000 Brussels - Belgium, **speak-up@bpost.be**

For Belgian subsidiaries of bpostgroup:

- **Speos:** HR director, HR department, Bollinckxstraat 24/32, 1070 Brussels - Belgium, **Hr@speos.be**
- **AMP :** CHRO, HR department, Lenniksebaan 451, 1 070 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.

3 Where and how can I report externally?

Concerns relating to bpost (company of public law) itself can be reported to the "federal Ombudsman", **https://www.federaalombudsman.be/fr**

Concerns relating to the Belgian private sector subsidiaries can be reported to the public authorities included in the Royal Decree of 22 January 2023 which appoints the competent authorities: **NL** / **FR**.

4 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.

0800 75 544

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 kept as long as it is needed to serve the purposes for which it is collected (the investigation). In case the investigation is followed by litigation, the data may be kept as long as it is necessary for the legal procedure.

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.

2 Who is the responsible local reporting manager?

For IMX:

HR department, 1110 bis Avenue du Général Leclerc, Bâtiment 18 – 1B, 93500 PANTIN – 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 2016on 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) (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,

Country annexes

Germany

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.

2 Who is the responsible local reporting manager?

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.

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?

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.

800 727 406

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?

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

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”).

Under Section 4.3 of this Policy, the wording of the first case when it is possible to publicly disclose a concern is changed to: “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?

All integrity violations: each act that threatens or violates the public interest and which:

1. does not comply with the code of conduct, or which may be in breach of the national or EU rules; and/or
2. entails a risk to life, safety, health, the environment; and/or
3. entails a serious breach of professional duty or good management of your entity.

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?.

For Radial EU:

HR Department, Industrieweg 18, 2850 Boom – Belgium.

3 Where and how can I report externally?

Not yet available.

4 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.

00 800 111 3819

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?.

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?

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 fixed duration for how long personal data can be kept for. However, personal data may be retained until the investigation is closed.

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.

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.

5 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)

5 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