

## Table of Contents

1	Purpose & Scope .....	2
2	Requirements .....	2
	2.1 Reporting a concern.....	2
	2.2 Receipt of Report and Investigation .....	3
	2.3 No Retaliation .....	4
	2.4 External Reporting .....	4
	2.5 Confidentiality .....	4
3	Definitions .....	5
4	Document Revision History.....	6
5	Country Sections .....	7
	5.1 Belgium.....	7
	5.2 Czech Republic.....	16
	5.3 Denmark .....	18
	5.4 France.....	20
	5.5 Germany .....	30
	5.6 Greece .....	35
	5.7 Hungary .....	37
	5.8 Ireland .....	41
	5.9 Italy.....	45
	5.10Netherlands .....	46
	5.11Poland.....	49
	5.12Portugal .....	53
	5.13Romania.....	55
	5.14Slovakia .....	58
	5.15Spain .....	62
	5.16Sweden .....	68
6	Translated Country Sections .....	72
	6.1 Belgium.....	72
	6.2 Polska .....	87



## EU Whistleblowing Policy

### 1 Purpose & Scope

This EU Whistleblowing Policy (the "**Policy**") provides information on the EU Whistleblowing Directive and how in certain circumstances, employees can choose to report and where appropriate, have their concerns investigated locally, rather than at a group level. This Policy is designed to supplement the End-to-End Concerns Management Process Standard (the "**End-to-End Concerns Policy**"). Where there is a conflict between the End-to-End Concerns Policy and this Policy, then this Policy will apply.

There are country sections included within this Policy, which provide additional guidance on how the Policy will apply in the specified country.

#### **What concerns does this Policy apply to in Europe?**

This Policy specifically covers reports made by employees, shareholders and others, employed or engaged by one of the entities listed in the country sections and relating to the following matters ("**Reports**"):

- Breaches of European Union Law (a "**Union Law Allegation**");
- The concerns listed in the country section; or
- Retaliation against employees or legal or natural persons connected with employees who make Reports or facilitate the making of Reports concerning Union Law Allegations.

This Policy **does not** govern individual employee grievances, complaints relating to job performance, or complaints related to the terms and conditions of employment, that are not by their nature complaints which relate to a potential integrity violation, unless otherwise provided by local regulations.

### 2 Requirements

#### 2.1 Reporting a concern

##### **Internal reporting using group resources:**

Reports may be made using the reporting channels identified in the End-to-End Concerns Policy. Reports made through those channels will be received and processed using group resources (being the Incident Classification Group ("**ICG**")). The ICG is comprised of the Security,

Investigations and Resilience team, HR and Legal, with other stakeholders such as Forensics, Tech and Compliance brought in where necessary to advise on specific concerns.

Internal reporting locally:

In addition to the methods provided in the End-to-End Concerns Policy, you can make a Report via the email address listed in the country section, in accordance with local reporting arrangements as set out in the relevant country section.

## **2.2 Receipt of Report and Investigation**

### **a) Making a report and acknowledgement**

Reports may be made to the channels set out in the End-to-End Concerns Policy or the method described in the paragraph above. If the reporter makes a Report that falls within scope of this Policy or a relevant country section, the Report will be acknowledged within seven days of the Report being made. If the reporter requests a physical meeting, this will be set up within a reasonable timeframe.

### **b) Investigation process**

Once a Report has been received, the reporter may be asked to provide further information in connection with the investigation process.

Depending on the nature of the Report, it may be appropriate for the concerns to be investigated by specialist functions within the wider Haleon global group, as permitted under local law.

### **c) Feedback**

Where possible, the reporter will be provided with feedback on the action envisaged or taken as follow-up to the Report, subject always to applicable legal and regulatory obligations. The reporter will typically receive feedback within three months of the Report being made.

## 2.3 No Retaliation

Consistent with the End-to-End Concerns Policy, the Company will not tolerate any Retaliation or attempted Retaliation by any other person or group, directly or indirectly, against anyone who, based on a reasonable belief, makes a Report or provides assistance to Human Resources, Legal, the Company's management or any other person or group, including any governmental, regulatory or law enforcement body, investigating or otherwise helping to resolve a Report.

The Company will also not tolerate Retaliation against

- third parties who confidentially support the reporter in a report in a work related context,
- individuals who are related to the reporter and who may suffer reprisals in a work related context, such as co-workers or relatives of the reporter, or
- legal entities that the reporter owns, where the reporter works, or to which the reporter is otherwise connected, within a work related context.

(together "**Facilitators**")

## 2.4 External Reporting

The Company encourages the reporter to use internal reporting procedures set out in the End-to-End Concerns Policy and the country sections attached to this Policy, to make a Report.

There may also be occasions where it is appropriate for the reporter to make a Report to an external body. If the relevant competent authority in the employee's country has set up an independent external reporting channel, the reporter may raise their concerns through those means as well. Details of the authorities competent to receive a Report will be set out in the country sections.

The Company strongly encourages the reporter to seek advice before reporting a concern to anyone external other than through the identified channels.

## 2.5 Confidentiality

Consistent with the End-to-End Concerns Policy, all investigations will be conducted in a confidential manner, so that information will be disclosed only as needed to facilitate review of the investigation materials or otherwise as required by law.

The reporter will usually be given the opportunity to check and rectify the transcript or minutes of any telephone call or meeting in which the reporter makes a Report.

All records relating to any Report and to the investigation and resolution thereof will be retained on a strictly confidential basis, as required under the Company's record retention schedules in effect from time to time.

### 3 Definitions

**European Union Law:** means European Union Law relating to (a) public procurement; (b) financial services, products and markets, and prevention of money laundering and terrorist financing; (c) product safety and compliance; (d) transport safety; (e) protection of the environment; (f) radiation protection and nuclear safety; (g) food and feed safety, animal health and welfare; (h) public health; (i) consumer protection; (j) protection of privacy and personal data, and security of network and information systems; (k) breaches affecting the financial interests of the European Union as referred to in Article 325 Treaty on the Functioning of the European Union ("**TFEU**") and as further specified in relevant European Union measures; and (l) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of European Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

**Retaliate / Retaliation:** means retaliation against persons who make Reports and Facilitators concerning Union Law Allegations including but not limited to: (a) suspension, lay-off, dismissal or equivalent measures; (b) demotion or withholding of promotion; (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training; (e) a negative performance assessment or employment reference; (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; (g) coercion, intimidation, harassment or ostracism; (h) discrimination, disadvantageous or unfair treatment; (i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that they would be offered permanent employment; (j) failure to renew, or early termination of, a temporary employment contract; (k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; (l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry; (m) early termination or cancellation of a contract for goods or services; (n) cancellation of a license or permit; (o) psychiatric or medical referrals.

## 4 Document Revision History

### REVISION (Principal changes from last revision)

**Type of Change:**  New  Administrative changes;  
 Technical changes impacting:  
 Roles and responsibilities  
 Process or activities

**Reason for Change** N/A

**Description of Change** N/A

Last updated: 31 October 2024

## 5 Country Sections

### 5.1 Belgium

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

#### **Who this section applies to locally**

This section is implemented in Belgium by a local legal entity with 50+ employees, i.e. Haleon Belgium NV, with registered office at Da Vincilaan 5, 1930 Zaventem, Belgium, VAT BE 0404.195.238, RPM/RPR Brussels ("**Haleon Belgium**").

This section applies to Haleon Belgium employees, but we also accept Reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Belgium or any other Haleon legal entity. The categories of person who may make Reports by virtue of their working or professional relationship, in addition to employees of Haleon Belgium, include independent contractors, any person working under the supervision and direction of contractors, sub-contractors, service providers, suppliers, directors, officers, shareholders, members of the administrative, management or supervisory bodies, non-executives, volunteers, trainees former employees (when the information was acquired during their employment relationship) or candidates (when they obtained the information as a result of the recruiting process). In addition, Haleon Belgium employees and third parties who have obtained information outside the context of a working or professional relationship with Haleon Belgium can also make an internal Report locally, provided that the Report relates to financial services, products and markets and the money laundering legislation (collectively "**Reporters**").

#### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of employees, shareholders and others, employed or engaged by one of the entities listed in the country sections and relating to the following matters:

- breaches relating to any violation of the legal or regulatory (Belgian) provisions or the directly applicable European provisions, as well as the provisions taken in execution of these provisions, specifically for: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transportation safety; (v) environmental protection; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and animal welfare;

(viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and the security of networks and network and information systems; (xi) the fight against tax fraud; (xii) the fight against social fraud;

- breaches affecting the financial interests of the Union; and
- breaches relating to the internal market.

Information of which the disclosure is prohibited because it is covered by national security ("*la sécurité nationale*" / "*nationale veiligheid*"), because it concerns classified information ("*informations classifiées*" / "*gerubriceerde gegevens*"), medical confidentiality ("*le secret médical*" / "*het medisch beroepsgeheim*"), because it is covered by the professional confidentiality of attorneys ("*informations et renseignements que les avocats reçoivent de leurs clients ou obtiennent au sujet de leurs clients*" / "*informatie en inlichtingen die advocaten ontvangen van hun cliënten of verkrijgen over hun cliënten*") or the confidentiality of judicial deliberations ("*le secret des délibérations judiciaires*" / "*geheimhouding van rechterlijke beraadslagingen*") is expressly excluded from the scope of this section, in accordance with the applicable legal conditions as listed in Article 5, §1 of the Act of November 28, 2022 on the protection of persons who report breaches of national or Union law within legal entities in the private sector ("**Belgian Whistleblowing Act**").

### **How to internally report a breach or concerns covered by this section locally**

In Belgium, employees may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and where appropriate investigated locally, please contact Mr Michaël Falcomer (email [Haleon.SpeakUp.Belgium@Haleon.com](mailto:Haleon.SpeakUp.Belgium@Haleon.com)) with your concern, who has currently been appointed as local report manager ("**Local Report Manager**"). In the event that the Local Report Manager is absent from work (e.g. due to holidays, sick leave), the Legal & Compliance Director will substitute him/her. A face-to-face meeting with the Local Report Manager (or the person delegated by him/her) will be arranged within a reasonable time if requested by you.

In the event that the Local Report Manager is conflicted or is the subject of the Report, the Report can be submitted, at your choice, through the reporting channels identified in the End-to-End Concerns Policy or by sending an email to the person who substitutes the Local Report Manager during his/her absence.

Haleon may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.



## **Reception and handling of internal Reports that have been made locally**

Upon receipt of the Report, the Local Report Manager will make a preliminary assessment as to whether the facts reported are within the material scope of this section, as well as the consistency and plausibility of the facts reported, and may request additional information from you if deemed necessary.

Once a Report is received and receipt has been acknowledged, the Local Report Manager will also assess whether the Report reveals a structural issue or an issue that affects two or more entities of the group and/or can only be effectively addressed with a cross-border approach that Haleon Belgium has not the power to apply in a view of ensuring the effectiveness of the EU Whistleblower Directive. To the extent this is the case, the Local Report Manager could either:

- Provide the Reporter with feedback setting out (to the extent applicable) in detail why it was not possible for the Local Report Manager to investigate and/or address the Report locally. The Local Report Manager will then explicitly recommend the Reporter to submit the Report directly through the reporting channels identified in the End-to-End Concerns Policy; or
- Request the Reporter's consent to share the Report with the appropriate group resources. Notwithstanding this, the Local Report Manager remains responsible and accountable for any internal Reports that have been made locally, including for maintaining confidentiality, giving feedback, and addressing the Report. In case the Reporter does not consent to the sharing of the Report with the appropriate group resources, the Local Report Manager will provide the Reporter with feedback as set out in the above paragraph.

## **Investigations of the Report and feedback to the Reporter**

The Local Report Manager will lead the investigation of the Report, establishing the necessary internal (and, to the extent the Reporter's consent was obtained, external) resources for the same as well as the persons who must have access to the Report and to the information obtained from the Report and from the internal investigation process (including personal data, such as the Reporter's identity).

Once the investigation is concluded, the corresponding actions will be adopted according to Haleon Belgium policies and procedures and applicable local law.

The Local Report Manager remains in charge of maintaining communication with the Reporter and, if deemed necessary, may request additional information from the Reporter on the Report.

In any event, the Local Report Manager will contact the Reporter in writing within three (3) months of the initial acknowledgement of receipt of the Report or, if no response is received, within three months of the expiration of a period of seven (7) calendar days following the Report, to respond to the investigative actions, providing summary information on the steps planned or taken to follow up on the complaint and address the alleged concern reported, all subject to Haleon Belgium's other obligations (e.g. confidentiality and personal data protection obligations).

## **Safeguards**

Once an in-scope Report has been submitted, the Reporter will benefit from the safeguards set forth in Chapters 6 and 7 of the Belgian Whistleblowing Act, regarding, among other things, non-retaliation and confidentiality.

## **External reporting locally**

Haleon Belgium strongly encourages Reports to be made internally so that any concerns can be resolved. However, should you decide to report your concerns externally in compliance with the applicable legal provisions, besides the federal coordinator, you can report to the relevant Belgian competent authorities, i.e.:

- the Federal Public Service Economy;
- the Federal Public Service Finance;
- the Federal Public Service Public Health, Food Chain Safety and Environment;
- the Federal Public Service Mobility and Transportation;
- the Federal Public Service Employment, Labour and Social Dialogue;
- the Programming Public Service for Social Integration, Poverty Reduction, Social Economy and Metropolitan Policy;
- the Federal Agency for Nuclear Control;
- the Federal Agency for Medicines and Health Products;
- the Federal Agency for the Safety of the Food Chain;
- the Belgian Competition Authority;
- the Data Protection Authority;
- the Financial Services and Markets Authority;
- the National Bank of Belgium;
- Belgian Audit Oversight Board;

- the authorities mentioned in article 85 of the law of September 18, 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash;
- the National Committee for the Security of Drinking Water Supply and Distribution;
- the Belgian Institute for Postal Services and Telecommunications;
- the National Institute for Health and Disability Insurance;
- The National Institute for the Social Security of the Self-employed;
- the National Employment Office;
- the National Social Security Office;
- the Social Intelligence and Investigation Service;
- the Autonomous Anti-Fraud Coordination Service; and
- the Shipping Control.

The way to make external reports can be found on the websites of the relevant competent authorities.

### **Personal data processing**

Any Reports received will be treated with appropriate confidentiality and comply with current privacy and data protection legislation in force in each relevant country from time to time, in particular Regulation (EU) 2016/679 (GDPR) and implementing national laws, in particular, the Belgian Data Protection Act of 30 July 2018 ("**Data Protection Laws**").

This section provides information with respect to the processing of personal data in relation to the local reporting channel for Belgium and is in addition and without prejudice to the information provided in Haleon's Worker Privacy Notice [Site de communication - Belgium & Luxembourg Employee PN 18 Jul 2022.pdf - Tous les documents \(sharepoint.com\)](#) as far as employees are concerned, and the general [Haleon Privacy Centre](#), as may be amended from time to time. In case of conflict between the information provided in this section and in the relevant data protection information notices identified above, this section shall prevail.

Please consult the relevant data protection information notices identified above for further information with respect to the processing of personal data by Haleon Belgium, in particular data recipients, transfers of personal data outside the EEA, your rights and how and who to contact to exercise them.

If you are the subject of a Report, you will be informed about the collection of your personal data in accordance with applicable local requirements. In

accordance with applicable law, such information can be delayed if this is necessary for investigatory or other evidentiary purposes.

## **1. Data controller**

Haleon Belgium acts as the controller of personal data collected and processed in relation to the local reporting channel for Belgium.

## **2. Processing purposes and legal bases**

The purposes of the data processing are (i) to assess the Reports received through the local reporting channel for Belgium, (ii) to carry out the necessary internal investigations (iii) to record the operation and effectiveness of the internal and local reporting channel, (iv) to comply with the Belgian Whistleblowing Act and to (v) adopt the necessary measures to address the Reports received.

The lawful bases for the processing of personal data received as a result of a Report or in the framework of a subsequent internal investigation are Article 6(1)(c) of the GDPR (the processing is necessary for compliance with the legal obligation to have an internal whistleblowing channel) and Article 6(1)(f) of the GDPR (the processing is necessary for the legitimate interests pursued by Haleon Belgium, which include investigating and taking appropriate action related to a potential violation of relevant laws and regulations and other in-scope matters, thereby ensuring compliance). When pursuing those legitimate interests, Haleon Belgium will balance them with the data subjects' interests and fundamental rights and freedoms in relation to the protection of the data subjects' personal data.

In exceptional circumstances, such as when Haleon Belgium intends to disclose the Reporter's identity to third parties, Haleon Belgium may process personal data on the basis of explicit consent.

Personal data relating to criminal convictions or offenses shall only be processed as specifically authorized by Union or Belgian law, in particular where it is necessary to manage Haleon Belgium's own litigations as per the Belgian Data Protection Act.

If a Report contains special categories of personal data, such data shall only be processed (i) if the processing is necessary for the performance of obligations and the exercise of specific rights of Haleon Belgium or the data subject in the field of labour law and social security and social protection law, to the extent permitted by Union or Belgian law or by a collective agreement under Belgian law providing adequate safeguards for the fundamental rights and interests of the data subject (Art. 9 (2) (b) GDPR), or (ii) if the processing is necessary for the establishment, exercise or defence of legal claims (Art. 9 (2) (f) GDPR).

If special categories of personal data or personal data relating to criminal convictions or offenses are included in a Report but are not clearly relevant to the reported matter, they will be deleted immediately and securely.

Automated decision-making, including profiling, does not take place in connection with the use of the local reporting channel for Belgium.

### **3. Categories of personal data processed**

The following categories of personal data may be collected and processed through the use of the local reporting channel for Belgium:

- the identity, functions and contact details of the Reporter, the subject(s) of the Report, and the persons involved in (and the persons identified in connection with) the processing of the facts reported and further investigation thereof;
- Breaches and related facts reported (including data relating to fraud or allegations of fraud, or other violations of the law, or relating to suspected or possible criminal offences), communications and information collected/reviewed in connection with the reporting and investigation of the facts reported (subject to applicable requirements under applicable law), and investigation report; and
- consequences of the investigation, including possible disciplinary measures as well as criminal allegations, prosecutions or convictions, as the case may be;
- protection of the relevant persons against retaliation;
- follow-up on the Report.

Non-use of the local reporting channel for Belgium does not entail any consequences and providing personal data is voluntary. Failing to provide personal data may, however, delay or make it impossible for Haleon Belgium to act upon any Report submitted but does not entail any other consequences.

The source from which personal data originates is typically from the individual to whom it relates (e.g. employees themselves) and personal data that Haleon Belgium receives in a permissible manner from publicly available sources and/or from third parties as further described below.

Haleon Belgium may collect personal data in the ways listed below:

- Collection of personal data directly from the data subject, such as through a Report or other forms of information data subjects provide to Haleon Belgium in connection with their employment;
- Collection of personal data during data subjects' activities in the course of their employment, such as through their performance and

interaction with other employees, customers, or other individuals;  
and

- Collection of personal data from other parties such as Reporters and other employees.

#### **4. Confidentiality**

Your identity will be processed in a confidential manner. This means that your identity will not be disclosed to anyone beyond the authorized staff members competent to receive or follow up on Reports, except where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, or with your explicit consent. This also applies to any other information from which your identity may be directly or indirectly deduced. In case of disclosures pursuant to a European Union or national law obligation in the context of investigations by national authorities or judicial proceedings, you shall be informed thereof beforehand, unless such information would jeopardise the related investigations or judicial proceedings.

#### **5. Retention periods**

Personal data which is manifestly irrelevant to the handling of a specific Report will not be collected or, if accidentally collected, will be deleted without undue delay. More generally, personal data will be kept for no longer than it is necessary and proportionate for the purpose for which it has been collected in compliance with applicable law and the Company's record retention schedules in effect from time to time.

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the Reporter, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations and the specific retention periods contained in the Belgian Whistleblowing Act as described below. In particular, personal data relating to out-of-scope Reports will be destroyed without undue delay.

In accordance with Article 22, §1 of the Belgian Whistleblowing Act, Reports will be kept for the duration of the work-related relationship of the Reporter with Haleon Belgium. The name, function and contact details of the Reporter and of any person to whom the protection and support measures under the Belgian Whistleblowing Act extend, as well as the subjects of the Report and any third parties mentioned in the Report, including, where applicable, their company number, will be saved until the reported violation is time-barred, as required under Article 21 of the Belgian Whistleblowing Act.

In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will in any event be retained until the end of the proceedings or the end of the limitation period for appeals against the decision.

Furthermore, Haleon Belgium may retain personal data relating to a Report for up to five (5) years, in intermediate storage, if it is legally obliged to do so (for example, to meet accounting, social or tax obligations)

## **6. Data protection rights**

Data subjects can exercise their rights of access, rectification, deletion, transfer (portability), limitation of the processing and objection as described in the relevant data protection information notices identified above. They also have the right to withdraw their consent at any time, and to file complaints with the competent data protection authority. In the case of Belgium, this is the Belgian Data Protection Authority (<https://www.dataprotectionauthority.be>).

## 5.2 Czech Republic

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in the Czech Republic by **Haleon Czech Republic s.r.o.**, having its registered office at Hvězdova 1734/2c, Nusle, 140 00 Prague 4, Identification No.: 036 55 067 ("**Haleon Czech**").

This section applies to Haleon Czech employees, but we also accept Reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Czech or any other Haleon legal entity. The categories of person who may make Reports by virtue of their working or professional relationship, in addition to employees of Haleon Czech, include independent contractors, sub-contractors, service providers, suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, job candidates, volunteers and trainees (collectively "**Reporters**").

### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters relating to the following matters:

- Violation which qualifies as a criminal offence;
- Violation which qualifies as an administrative offence punishable by a fine with upper limit of at least CZK 100,000;
- Violation of the Czech Whistleblowing Act;
- Violation of the Czech legal regulation in the areas specified in the definition of the European Union Law.

### **How to internally report a breach or concerns covered by this section locally**

In the Czech Republic, Reporters may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and where appropriate investigated locally, please contact the following designated person/s: Lucie



Nezkusilova, +420702203133, [lucie.x.nezkusilova@haleon.com](mailto:lucie.x.nezkusilova@haleon.com) with your concern.

Haleon may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.

#### External reporting locally

Haleon Czech strongly encourages Reports to be made internally so that any concerns can be resolved. However, should Reporters decide to report their concerns externally, the competent authority is set out below:

- the Ministry of Justice (*Ministerstvo spravedlnosti*, <https://oznamovatel.justice.cz/>).

#### **What to expect when reporting a concern locally**

In addition to the information provided in the Policy, please note that:

- If requested by the Reporter, the designated person must allow a personal filing of the Report within 14 days.
- The designated person must confirm the receipt of the Report in writing, within 7 days. Furthermore, the designated person shall inform the Reporter of any action taken, the status of the internal investigation as well as the outcome thereof within a reasonable period of time, but no later than 30 days from the confirmation of receipt. In the event of factually or legally complex cases, this period may be extended once or at most twice with each extension lasting up to 30 days. The designated person is obligated to inform the Reporter in writing of the extended deadline and the reasons for its extension before the deadline expires.

#### **Archiving of Report and handling of personal data**

The personal data is processed while the case is ongoing and for a period of 5 years from the date of receipt of the Report.

You also have the right to complain about the processing of personal data to your local supervisory authority, which in the Czech Republic is the Office for Personal Data Protection, [www.uoou.cz](http://www.uoou.cz).

### 5.3 Denmark

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

#### **Who this section applies to locally**

This section is implemented in Denmark by local legal entities with 50+ employees ("**Haleon Denmark** ").

This section applies to Haleon Denmark employees ("**Reporters**").

#### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters relating to the following matters:

- violations of specific areas of the EU law, as referred to in this Policy; and
- serious offences and other serious matters, which may relate to:
  - Punishable offences, e.g., abuse of funds, theft, fraudulent misrepresentation, embezzlement, fraud, bribery, etc;
  - Serious or repeated violations of Danish legislation;
  - Serious or repeated violations of material internal guidelines, e.g., on business trips, gifts, financial reporting, etc; and / or
  - Serious workplace conflicts, e.g., in the form of sexual harassment or other serious harassment.

#### **How to internally report a breach or concerns covered by this section locally**

In Denmark, employees may use the reporting channels identified in the End-to-End Concerns Policy. However, using the channels in the End-to-End Concerns Policy means the concern will be heard and potentially investigated outside of the whistleblower system described in this section and the requirements in the Danish Whistleblower Act and instead in accordance with the End-to-End Concerns Policy using group resources and as such, the Report may not be dealt with confidentially.

If you wish to have the Report heard and where appropriate investigated locally in accordance with the confidentiality requirements set out in this section and the requirements in the Danish Whistleblower Act, please email [Haleon.SpeakUp.Denmark@Haleon.com](mailto:Haleon.SpeakUp.Denmark@Haleon.com) with your concern.

The Report will be acknowledged within seven days of the Report being made. If the Reporter requests a physical meeting, this will be set up within a reasonable timeframe.

Haleon may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.

### **Duty of confidentiality**

The designated persons at Haleon Denmark are appointed to receive and investigate Reports received, are subject to a special duty of confidentiality. Further, any person at Haleon Denmark or at group level who is involved in the investigations of a Report will be subject to the same special duty of confidentiality with regard to any information that has or is subject of the investigation of the Report received.

Information that may directly or indirectly disclose the Reporter's identity will not be shared with any who are not a designated at Haleon Denmark to receive and investigate Reports without the Reporter's explicit consent.

### **Notice to reported persons and to other persons**

If information about you is reported in a Report received, and the Report falls within this section, you will as a general rule, not receive any information about the processing of your personal data.

If, on the other hand, the Report does not fall within this section, you will be informed of the processing of your personal data in accordance with the rules of the Data Protection Regulation and the Danish Data Protection Act.

### **Data protection**

The processing of personal data in connection with a Report received will be on the basis of section 22 of the Danish Whistleblower Act, according to which processing of personal data subject to articles 6, 9 and 10 of the General Data Protection Regulation may take place if the processing of the personal data is necessary to investigate a Report received in a whistleblowing system established in accordance with the Danish Whistleblower Act.

For further information with regard to the processing of personal data please refer to the Denmark Privacy policy for employees or Privacy policy for external parties ([www.privacy.haleon.com/da-dk/general/](http://www.privacy.haleon.com/da-dk/general/)).

### **External reporting locally**

Haleon Denmark strongly encourages Reports to be made internally so that any concerns can be resolved. However, should employees decide to report their concerns externally, the competent authority is set out below:

- The Danish Data Protection Agency's general external whistleblowing system ([www.whistleblower.dk](http://www.whistleblower.dk)).

## 5.4 France

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

This country section is implemented in France by local legal entities with 50+ employees ("**Haleon France**").

### Who this section applies to locally

The following individuals are encouraged to use the internal reporting process ("**Individuals**"):

- all current Haleon France employees, former Haleon France employees where the information was obtained in the course of that relationship, and individuals who have applied for employment with Haleon France, where the information was obtained in the course of that application;
- shareholders, partners and holders of voting rights in the general meeting of the entity;
- members of the administrative, management or supervisory body ("aux membres de l'organe d'administration, de direction ou de surveillance");
- external and occasional consultants;
- contractors of the entity concerned, their subcontractors or, where the contractor is a legal entity, members of the administrative, management or supervisory bodies of these contractors and subcontractors, as well as members of their staff.

The Individuals, who have obtained, in the course of their professional activities, information related to the wrongdoings that may be reported as provided by the applicable law, relating to facts which have occurred or are very likely to occur in the entity concerned, may report such information internally in accordance with the applicable procedures, in particular where the Individuals consider that it is possible to remedy the breach effectively by this reporting and that they do not expose themselves to a risk of retaliation.

### What concerns does this section apply to locally

Under French law, the whistleblower is the individual ("*personne physique*") who reports or discloses, without direct financial consideration and in good faith, information relating to ("**Reports**"):

- a crime, an offence, a threat or harm to the general interest,
- a violation or an attempt to conceal a violation of an international commitment regularly ratified or approved by France, a unilateral act of an international organization taken on the basis of such a commitment,
- the European Union Law,
- the law or regulations.

Facts / information / documents, regardless of their form or medium, the disclosure of which is prohibited because they are covered by national security ("*secret de la défense nationale*"), medical secrecy ("*secret médical*"), secrecy of judicial deliberations, judicial investigations or judicial enquiries ("*au secret des délibérations judiciaires, au secret de l'enquête ou de l'instruction judiciaires*"), or legal professional secrecy ("*secret professionnel de l'avocat*") are expressly excluded from the whistleblowing scheme.

Haleon France may process personal data for the purpose of providing the Policy and to investigate Reports, according to (i) its obligation to comply with legal provisions regarding the implementation of a whistleblowing system; and (ii) its legitimate interests in ensuring that employees comply with applicable law and its policies and procedures. When pursuing those legitimate interests, Haleon France will balance them with the Individual's interests and fundamental rights and freedoms in relation to the protection of the Individual's personal data.

The following categories of personal data may be collected and processed as part of the investigation of Reports:

- Identity, functions and contact details of the whistleblower;
- Identity, functions and contact details of the persons who are the subject of the Report;
- Identity, functions and contact details of persons involved in the collection or processing of the Report;
- Facts reported;
- Elements collected within the framework of the verification of the reported facts;
- Investigation reports; and
- Follow-up to the Report.

Special categories of personal data (including personal data relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, sexual life or orientation), as well as personal

data relating to criminal convictions or offenses may be processed as part of the handling of a Report when their processing is necessary to the establishment, exercise or defense of legal claims.

Haleon France endeavors to process only the data necessary for the purposes of investigating Reports. To that end, whistleblowers are invited to ensure that any information communicated when making a Report remains factual and directly relevant to the subject of the Report.

### **How to internally report a breach or concerns covered by this section**

In France, Individuals may submit a Report through the reporting channels identified in this France country section.

#### ***Internal reporting using group resources:***

Reports may be made using the reporting channels identified in the End-to-End Concerns Policy. Reports made through those channels will be received and processed using group resources (being the Incident Classification Group ("**ICG**"). The ICG is comprised of the Security, Investigations and Resilience team, HR and Legal, with other stakeholders such as Forensics, Tech and Compliance brought in where necessary to advise on specific concerns.

#### ***Internal reporting locally:***

If you choose to follow the local speak up process rather than the group resources, please email [Haleon.SpeakUp.France@Haleon.com](mailto:Haleon.SpeakUp.France@Haleon.com). This will be monitored by Marie-Maud Danmanville (in-country Compliance Officer) (hereafter the "**Local Reports Referent**").

When making a Report, the Individual is encouraged to provide:

- any evidence, whatever its forms, likely to support the Report; and
- anything demonstrating that the evidence belongs to the Individual (except in case of a Report made anonymously).

Haleon France will ensure that the Local Reports Referents are able to perform their duties in respect to this procedure in an impartial manner, by providing the following guarantees:

- the Local Reports Referents will be free to treat Reports under the terms of this procedure without the need for management approval;
- the Local Reports Referents will not be subject to retaliation for performing their duties under the terms of this procedure;

- the Local Reports Referents are individuals who, by virtue of their position or status, have the competence, authority and means to carry out their duties;
- the Local Reports Referents shall handle all reports in accordance with applicable legal requirements;
- the Local Reports Referents must conduct any investigation in accordance with the adversarial principle and with an impartial ear;
- the Local Reports Referents must immediately report to management any conflict of interest or other situation that may affect their impartiality.

The receipt of the Report will be acknowledged within seven (7) working days ("*jours ouvrés*") of receipt.

As part of this Policy, personal data acquired by Haleon France may transfer outside of the European Economic Area. To provide an adequate level of data protection for the transfer of personal data through the whistleblowing system, Haleon France has entered into an agreement including the European Commission's standard contractual clauses with the relevant entities of the relevant entities of the Haleon group. The Individual can obtain a copy of such standard contractual clauses by contacting us at [privacy@haleon.com](mailto:privacy@haleon.com)

### **Anonymity and Confidentiality**

Reports may be made anonymously or on an open basis. However, we strongly encourage Reports to be made on an open basis, where possible. Anonymous reporting may limit the extent to which we are able to fully investigate Reports and take remedial action.

A Report made on an anonymous basis will be investigated, provided that:

- the seriousness of the alleged facts is evidenced and the factual elements supporting the claim are sufficiently detailed;
- anonymous Reports are handled with increased caution. For example, the first recipient of the Report may assess whether such anonymous Report should be processed through the whistleblowing system.

Whether the Report is made anonymously or on an open basis, the identity of the whistleblower will be processed in a confidential manner, in accordance with this France country section.

Other than in the circumstances identified in this France section, the identity of the Individuals may only be communicated with his/her

consent, except in cases where communication of this information to judicial authorities is mandatory.

The identity of the person who is the subject of the Report as well as the identity of any third party mentioned in the Report will also be processed in a confidential manner, in accordance with this section. The identity of the person who is the subject of the Report may only be communicated if the Report is well founded, subject to cases where communication of this information to judicial authorities is mandatory.

Haleon France prohibits access to information contained in a Report, including the identity of the Individual, the person(s) targeted in the Report and any third party referred to in the Report, to staff members who do not have authority to access this information.

Retaliation against those making Reports, whether direct or indirect, and persons who facilitate or otherwise assist in good faith in the making of the Report or the investigation process will not be tolerated.

### **Investigation process**

If the Individual makes a Report using the usual group resources, the ICG will carry out an assessment to determine the scope of any investigation. If the Individual makes a Report locally, the Report will be shared with an external law firm to obtain advice as to how to proceed in accordance with local legislation.

Individuals may be asked to provide further information in connection with the investigation process.

If applicable, the Individual will be informed of the reasons why the ICG considers that the Report does not meet the statutory conditions. If the Report is not admissible, any information and/or data provided by the Individual will be immediately destroyed.

Reports will be shared with the ICG in compliance with applicable information-sharing provisions.

The persons or services involved in the investigation process have, by virtue of their position or status, the competence, the authority and means necessary to carry out their missions.

### **Feedback**

The Local Reports Referents shall, within a reasonable period of time not exceeding three (3) months as from the acknowledgment of receipt of the alert or, if no acknowledgment is received, three (3) months as from the expiry of a seven (7)-working day period following the reporting of the Report, provide the Individual with written information on the



measures envisaged or taken to assess the accuracy of the allegations and where appropriate, to remedy to the issues provided in the Report, as well as the reasons for such measures.

Haleon France shall close the Report when the allegations are inaccurate or unfounded or when the Report has become irrelevant. The Individual should then be informed in this respect in writing.

### **Record keeping**

Reports made orally (e.g., by voice message to the toll-free telephone number) will be recorded as follows:

- If the Report is collected on the recorded telephone line or other recorded voice mail system, with the consent of the Individual: Haleon France will either (i) record the conversation on a durable and retrievable medium or (ii) transcribe the entire conversation;
- If the Report is collected over the unrecorded telephone line or other unrecorded voice mail system: Haleon France will make an accurate written transcript of the conversation; and
- If the Report is collected during a videoconference or physical meeting, with the consent of the Individual: Haleon France will either (i) record the conversation on a durable medium or (ii) make an accurate written transcript of the conversation.

The Individual will have the opportunity to verify, rectify and approve the transcript of the conversation or the minutes (as applicable) by signing them.

The recordings, transcripts and minutes shall be kept only as long as is strictly necessary and proportionate for the processing of the Report and for the protection of the Individual(s), the persons targeted and the third parties mentioned therein.

Reports will only be kept for as long as it is strictly necessary and proportionate for their investigation and for the protection of the Individuals, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations.

In particular, personal data relating to out-of-scope Reports will be destroyed without delay or anonymized.

If no action is taken following an in-scope Report, the personal data relating to this Report will be destroyed or anonymized by Haleon France within two (2) months of the end of the investigation.

In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will be retained until the end of the proceedings or the end of the limitation period for appeals against the decision.

Further, Haleon France may retain personal data relating to a Report for up to five (5) years, in intermediate storage, if it is legally obliged to do so (for example, to meet accounting, social or tax obligations).

### **External reporting locally**

Haleon France strongly encourages Reports to be made internally so that any concerns can be resolved. However, should employees decide to report their concerns externally in compliance with applicable provisions, the competent authorities are set out below:

- the competent authorities listed in annex of the Decree n°2022-1284 dated 3 October 2022 (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046357368>);
- the administrative body "Défenseur des droits";
- the judicial authority;
- an institution, body or agency of the European Union empowered to collect information on violations falling within the scope of the European directive dated 23 October 2019.

The Report may only be made public by the Individual:

1. after having been raised internally and/or externally without any appropriate measures being taken after the expiration of specific time limits:
  - for the competent authorities as listed in the annex of the Decree n°2022-1284 dated 3 October 2022, within a reasonable period of time not exceeding three (3) months as from the acknowledgement of receipt of the alert, or in the absence of acknowledgement of receipt, three (3) months as from the expiry of a period of seven (7) working days following the alert. This period is extended to six (6) months if the particular circumstances of the case, linked in particular to its nature or complexity, require further diligence, in which case, the authority must justify these circumstances to the author of the alert before the expiration of the three (3) - month period mentioned above; or
  - for the administrative body "*Défenseur des Droits*", the judicial authority or a competent EU institution, body or agency, within six (6) months as from the acknowledgement of receipt of the

alert, or in the absence of acknowledgement of receipt, within six (6) months from the expiry of a period of seven (7) working days following the Report;

2. in case of serious and imminent danger, or in case of imminent or obvious danger to the public interest, especially when there is an emergency situation or a risk of irreversible harm, or
3. when referring the matter to the competent public authority would put the author at risk of retaliation or would prevent the content of the disclosure from being remedied effectively, due to the specific circumstances of the case, in particular if evidence may be concealed or destroyed or if the Individual has serious grounds for believing that the authority may have a conflict of interest, be in collusion with the author of the facts or be involved in those facts.

### **Protection against retaliation**

Individuals benefit from the protection provided for by applicable French statutory provisions.

In particular, Individuals are protected against any form of (threats and attempts of) retaliation (including termination, demotion, suspension, loss of benefits, threats, harassment or discrimination). Retaliation and reprisals by Haleon France or its employees against colleagues are a serious and material breach of this procedure.

Haleon France seeks to protect Individuals from retaliation and reprisals, and Haleon France will take appropriate disciplinary action against any employee who engages in retaliatory conduct. Conversely and for the avoidance of doubt, making a Report in bad faith or abusive use of reporting channels otherwise could lead to disciplinary sanctions, up to and including dismissal.

When a Report or public disclosure has been made anonymously, the individual whose identity is subsequently revealed has the same protections as any Individuals.

### **Privacy Rights**

Pursuant to applicable law, the Individual has the right to: (a) request access to their personal data; (b) request rectification of their personal data; (c) request erasure of their personal data ("the right to be forgotten"); (d) request restriction of processing of their personal data; and (e) object to the processing of their personal data while Haleon France verifies their processing.

The above rights may not be used by the person who is the subject of a Report to obtain information relating to the identity of the whistleblower.

**More on the right of access:** The right to access personal data includes the right to receive a copy of all, or a portion, of the Individual's personal data in Haleon France's possession as long as Haleon France providing personal data would not adversely affect the rights and freedoms of others. In any case, the Individual will not be granted access to the personal data of third parties.

**More on the right to rectification:** The exercise of such right may not result in the retroactive modification of the elements contained in a Report or collected during the investigation. When exercised, this right must not make it impossible to reconstruct the chronology of any changes of important elements of the investigation. This right can only be exercised to rectify factual data.

**More on the right to object:** The Individual has the right to object to the processing of their personal data based solely on Haleon France's legitimate interests on grounds relating to their particular situation. If the Individual does object in these circumstances, the processing of their personal data will be stopped unless there is an overriding, compelling reason to continue the processing or the processing is necessary to establish, pursue or defend legal claims.

The Individual also has the right to define directives concerning the conservation, deletion and communication of their personal data after their death.

The Individual can exercise these rights by submitting an email to [Haleon Privacy Web Form \(onetrust.com\)](mailto:Privacy@haleon.com) Haleon France will respond to such requests in accordance with applicable data protection law.

If the Individual believes that their personal data has been processed in violation of applicable data protection law, they have the right to lodge a complaint with the Commission Nationale de l'Informatique et des Libertés ("CNIL"), located at:

3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07

France

For more information about the processing of personal data, please refer to Haleon France's [Legal & Compliance Hub - France Employee PN 18 Jul 2022.pdf - All Documents \(sharepoint.com\)](#)

For any questions about this Policy, please contact: Hannah.c.Boast@haleon.com or Jules.m.parke-robinson@haleon.com.



## 5.5 Germany

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail. For a Report to be in scope of the procedure outlined below, the Reporter has to report a potential Breach to the local internal reporting channel outlined below.

This country section is implemented in Germany by local legal entities with 50+ employees ("**Haleon Germany**").

### **Who this section applies to locally**

This section applies to Haleon Germany employees reporting Breaches in accordance with b) to reporting channels defined under c) as well as leased employees, persons employed for the purpose of their vocational training and persons who, due to their economic independence, are to be regarded as equivalent to employees but we also accept reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Germany or any other Haleon legal entity. The categories of person who may make reports by virtue of their working or professional relationship, in addition to employees of Haleon Germany, include candidates, former employees, independent contractors, consultants, paid and unpaid volunteers and trainees and shareholders and persons with administrative, management, control, supervisory or representative functions, as well as persons whose legal relationship with Haleon Germany still has not started, those whose probationary period is still ongoing and those whose legal relationship with Haleon Germany has terminated (collectively "**Reporters**").

### **What concerns do this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers the reporting of complaints and concerns (collectively, "**Reports**") relating to the following matters:

- violations that are subject to criminal liability (*Verstöße, die strafbewehrt sind*)
- violations which are subject to administrative fines (*Verstöße, die bußgeldbewehrt sind*) provided the violated regulation serves to protect life, limb or health or to protect the rights of employees or their representative bodies
- Offences of federal and state legislation related to: (i) public procurement; (ii) financial services, products and markets, and/or prevention of money laundering and/or terrorist financing; (iii) product safety and/or compliance; (iv) transportation safety; (v)

environmental protection; (vi) radiation protection and/or nuclear safety; (vii) food and/or food safety, animal health and animal welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and/or personal data and/or the security of networks and/or network and information systems;

- Offences affecting the financial interests of the European Union, such as breaches of the relevant anti-fraud or anti-corruption legislation;
- Offences relating to the internal market, in particular breaches of the rules on competition and/or State aid

(together, the "**Breaches**").

This section does not cover reports relating to the reporter's own personal circumstances, grievances, complaints or employment relationship. Such concerns will generally fall outside the scope of this section and it may be more appropriate to raise such matters under a different global or Haleon Germany policy or procedure.

Facts / information / documents, regardless of their form or medium, the disclosure of which is prohibited because they are covered by national security, medical secrecy, secrecy of judicial deliberations, or legal professional secrecy are expressly excluded from the whistleblowing scheme.

### **How to internally report a Breach or concerns covered by this section locally**

In Germany, the Reporter may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and investigated locally, please email [Haleon.SpeakUp.Germany@Haleon.com](mailto:Haleon.SpeakUp.Germany@Haleon.com) with your concern. Reports via [Haleon.SpeakUp.Germany@Haleon.com](mailto:Haleon.SpeakUp.Germany@Haleon.com) will be received and potentially investigated by the GER Reporting Team.

The receipt of the Report will be acknowledged within seven (7) working days of receipt.

### **Investigation process and feedback**

Once a Report has been received, the GER Reporting Team will carry out an initial assessment to determine whether there is *prima facie* evidence of a Breach and, if so, appropriate action will be taken which may include an investigation. The Reporter may be asked to provide further information in connection with any such investigation process.

Furthermore, Haleon may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation or may involve other forensic third-party providers to assist with an investigation if required, who will be under confidentiality obligations.

Haleon will aim to keep the Reporter informed of the progress of any investigation and its likely timescale. However, sometimes the need for confidentiality may prevent us from giving the Reporter specific details of the investigation or any action taken as a result. The Reporter is required to treat any information about the investigation as strictly confidential.

If and to the extent Reporters can be contacted, they will be provided with feedback within three months of acknowledgment of receipt of the Report (or, if no acknowledgment is received, three months from the expiration of a period of seven calendar days following receipt of the Report). The feedback includes the communication of planned as well as already taken follow-up actions and the reasons for them. Sometimes the need for confidentiality may prevent us from giving the Reporter specific details of the investigation or any action taken as a result.

### **Anonymity and Confidentiality**

Reports may be made anonymously or on an open basis. However, we strongly encourage Reports to be made on an open basis, where possible. Anonymous reporting may limit the extent to which we are able to fully investigate Reports and take remedial action.

Haleon will take steps to maintain confidentiality for all parties involved. The Reporter's identity as well as the identity of the person who is subject of the Report, any third party mentioned in the Report and any information received in connection with the Report form which the identity may be directly or indirectly deduced will be processed in a confidential manner in accordance with applicable law.

Retaliation against those making Reports, whether direct or indirect, and persons who facilitate or otherwise assist in the making of the Report or the investigation process will not be tolerated.

### **Malicious or False Reports**

If it is found that a person knowingly reported false information or that a Report of wrongdoing was made maliciously, the person who made the Report may be subject to disciplinary action.

### **Record keeping**

Reports made orally (e.g., by voice message to the toll-free telephone number) will be recorded as follows:



- If the Report is collected on the recorded telephone line or other recorded voice mail system, with the consent of the Individual: Haleon will either (i) record the conversation on a durable and retrievable medium or (ii) transcribe the entire conversation;
- If the Report is collected over the unrecorded telephone line or other unrecorded voice mail system: Haleon will make an accurate written transcript of the conversation; and
- If the Report is collected during a videoconference or physical meeting, with the consent of the Individual: Haleon will either (i) record the conversation on a durable medium or (ii) make an accurate written transcript of the conversation.

The Individual will have the opportunity to verify, rectify and approve the transcript of the conversation or the minutes (as applicable) by signing them.

The documentation has to be deleted three years after the investigation procedure is completed. The documentation may be retained longer in order to comply with requirements under the German Legislation or other legislation as long as this is necessary and proportionate.

### **External reporting locally**

Haleon strongly encourages Reports to be made internally so that any concerns can be resolved. However, should employees decide to report their concerns externally in compliance with applicable provisions, the competent authorities are set out in the Whistleblower Protection Act (*Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden*). In particular, the local external reporting channels can be found [here](#). The Reporter may also make a Report to institutions, bodies, offices or agencies of the European Union, such as:

European Commission

European Anti-Fraud Office (OLAF)

European Maritime Safety Agency (EMSA)

European Union Aviation Safety Agency (EASA)

European Securities and Markets Authority (ESMA)

European Medicines Agency (EMA)

## **Protection against retaliation**

Individuals benefit from the protection provided for by applicable German statutory provisions.

Specifically, the protection against retaliation applies to:

- the Reporter and
- Facilitators, i.e.:
  - third parties who confidentially support the Reporter in a Report in a work related context,
  - individuals who are related to the Reporter and who may suffer reprisals in a work related context, such as co-workers or relatives of the Reporter, or
  - legal entities that the Reporter owns, where the Reporter works, or to which the Reporter is otherwise connected, within a work related context.
- (collectively "**Individuals**")

In particular, Individuals are protected against any form of (threats and attempts of) retaliation (including termination, demotion, suspension, loss of benefits, threats, harassment or discrimination). Retaliation and reprisals by Haleon or its employees against colleagues are a serious and material breach of this procedure.

Haleon seeks to protect Individuals from retaliation and reprisals, and Haleon will take appropriate disciplinary action against any employee who engages in retaliatory conduct.

When a Report or public disclosure has been made anonymously, the individual whose identity is subsequently revealed has the same protections as any Individuals.

## 5.6 Greece

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Greece by the local legal entity by local legal entities with 50+ employees ("**Haleon Greece**").

This section applies to Haleon Greece employees, but we also accept Reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Greece or any other Haleon legal entity. The categories of person who may make Reports by virtue of their working or professional relationship, in addition to employees (full or part-time, indefinite or fixed term, posted, etc.) of Haleon Greece, include the following: self-employed persons, consultants and home workers, shareholders, any person working under the supervision and direction of contractors, sub-contractors, and suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, volunteers and (paid or unpaid) trainees. Also, Reports can be made by persons, who obtained information on breaches, in the framework of their employment which has ended (for any reason, including retirement), as well as persons whose employment relationship has not yet begun, where information on breaches has been acquired during the recruitment process or during other precontractual negotiations (collectively "**Reporters**").

### **How to internally report a breach or concerns covered by this section locally**

In Greece, employees may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and where appropriate investigated locally, please email [Haleon.Speakup.Greece@Haleon.com](mailto:Haleon.Speakup.Greece@Haleon.com) with your concern.

Haleon may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.

### **Personal Data Processing**

The personal data processed in the context of a Report pursuant to the Policy shall be processed in compliance with applicable data protection legislation, including the EU Regulation 679/2016 ("**GDPR**") and Greek law 4624/2019.

As a matter of exception from the general GDPR rules, Haleon Greece will not inform the person who is referred to in the Report as a person to whom the breach is attributed or any third party mentioned in the Report regarding their personal data processing and may not satisfy their relevant rights (right to access, rectification, erasure, etc.), as long as this is necessary to prevent attempts to obstruct the Report, to protect the investigation, to protect the Reporter's identity, and to protect the Reporter from any form of retaliation.

### **External reporting locally**

Haleon Greece strongly encourages Reports to be made internally so that any concerns can be resolved. However, should employees decide to report their concerns externally, the competent authority is the National Transparency Authority (the "**NTA**"). Reports can be made directly to the NTA, as set out below:

- Electronically: Via the dedicated electronic platform of the NTA, available here: <https://extwhistle.aead.gr>.
- In writing: in person or by post at the headquarters of the NTA, in an envelope marked "External report under Law 4990/2022" or bearing another indication that the Report falls within the provisions of the Law, concerning the external channel of the NTA, or by email at the following email address: [external.whistle@aead.gr](mailto:external.whistle@aead.gr).
- Orally: by means of a physical meeting with the authorised Inspector-Auditor upon your request submitted at [external.whistle@aead.gr](mailto:external.whistle@aead.gr) or by phone call on the telephone line (+30) 2132129900 (Monday – Friday 9:00 a.m. to 2:00 p.m.). In this case, the Report will be recorded.

## 5.7 Hungary

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Hungary by local legal entities with 50+ employees ("**Haleon Hungary**").

The following individuals associated with Haleon Hungary are encouraged to use the internal reporting process:

- Current employees of Haleon Hungary;
- Employees whose employment relationship was terminated with Haleon Hungary;
- Persons seeking to establish an employment relationship with Haleon Hungary, provided that the procedure for establishment has been started;
- Any self-employed person who has a contractual relationship with Haleon Hungary;
- Persons who have ownership in Haleon Hungary as a company and/or who are members of the administrative, executive or supervisory body of Haleon Hungary;
- Persons who have initiated the procedure for establishing a contractual relationship with Haleon Hungary or who is or has been a contractor, subcontractor, supplier or person under the supervision and direction of such contractor;
- Trainees and volunteers working for Haleon Hungary;
- Persons who wish to enter into a legal or contractual relationship with Haleon Hungary within the meaning of points (d), (e) or (g) and for whom the procedure for the establishment of such a legal or contractual relationship has been initiated; and
- Persons who ceased to have a legal or contractual relationship with Haleon Hungary within the meaning of points (d), (e) or (g).

Collectively ("**Reporters**")

### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of employees, shareholders and others, employed or engaged by one of the entities listed

in the country sections and relating to any unlawful or suspected unlawful act or omission or other abuse ("**Breach**").

### **How to internally report a breach or concerns covered by this section locally**

In Hungary, employees may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and where appropriate investigated locally, please email, call or contact personally Ms. Szedmák Nóra, HR Generalist, (Haleon Hungary Kft. 1124 Budapest, Csörsz u. 43.; Email [nora.x.szedmak@haleon.com](mailto:nora.x.szedmak@haleon.com); Mobile +36 70 653 0746 ("**Local Reporting Contact**") with your concern.

Haleon Hungary may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.

### **External reporting locally**

Haleon Hungary strongly encourages Reports to be made internally so that any concerns can be resolved. However, should employees decide to report their concerns externally, the competent authorities are set out below:

- Directorate General for the Auditing of European Funds (<https://eutaf.kormany.hu/>)
- Hungarian Competition Authority (<https://www.gvh.hu/>)
- Integrity Authority (<https://integritashatosag.hu/>)
- Public Procurement Authority (<https://www.kozbeszerzes.hu/>)
- Hungarian Energy and Public Utility Regulatory Office (<https://www.mekh.hu/>)
- National Bank of Hungary (<https://www.mnb.hu/>)
- National Authority for Data Protection and Freedom of Information (<https://www.naih.hu/>)
- National Media and Infocommunications Authority (<https://nmhh.hu/>)
- Hungarian Atomic Energy Authority (<https://www.haea.gov.hu/>)
- Supervisory Authority of Controlled Activities (<https://sztfh.hu/>)
- Office of the Commissioner for Fundamental Rights of Hungary (<https://www.ajbh.hu/>)

- Competent institutions, bodies, offices or agencies of the European Union.

We encourage you to keep yourself updated of the latest regulations of the Hungarian Government. The Hungarian Government may unilaterally designate other organizations and/or authorities in the future which should be considered to be an external reporting channel.

## **Investigation**

The Report will be assessed by the Local Reporting Contact. If the Report contains valid reference to a Breach, it will be appropriately investigated by Ms. Renáta Pukanová, HR Business Partner Romania, Hungary, Czech Republic, Slovakia (Email: [renata.8.pukanova@haleon.com](mailto:renata.8.pukanova@haleon.com); Tel: +421 903 606 552) ("**Case Manager**"). If the Report is not qualified as a valid Report, the Report will be closed or waived, and the Reporter will be informed in writing.

According to the Whistleblowing Act, the investigation of a Report may be waived if:

- the Report was made anonymously;
- the Report was not filed by a person entitled to do so;
- the Report is a repeated Report by the same Reporter with the same content as the previous Report; or
- the prejudice to the public interest or to an overriding private interest would not be proportionate to the restriction of the rights of the natural or legal person (i.e. the person concerned by the notification) resulting from the investigation of the Report.

## **Feedback**

The Reporter will typically receive feedback within thirty days of the Report being made. The 30-days deadline may be extended to not more than 3 months on a duly justified basis, of which the Reporter shall be notified at the same time.

## **Confidentiality**

### **A) Anonymity and Confidentiality of the Reporter**

#### **Anonymity**

When reporting a Breach, the Reporter may choose to do so anonymously. However, according to the Hungarian Whistleblowing Act, the investigation of a Report may be waived if it was submitted anonymously.

## **Confidentiality**

The identity of the Reporter is kept confidential and may only be accessible to the restricted list of persons involved in the case management (subject to obligations arising from the law or the applicable legal proceedings), e.g., the Case Manager, the appointed investigator(s), and any external or internal person mandated to support the investigation or next steps following the closing of the case. No one else will be informed.

The identity of the Reporter must be kept confidential at any circumstances (regardless of the job position or seniority in Haleon Hungary) and, if necessary for the investigation to inform another person, the Case Manager should be consulted and approve. An unauthorized disclosure may lead to disciplinary actions.

In all cases, the identity of the Reporter will not be provided to the reported person, unless expressly agreed by the Reporter or required by law or in the framework of legal proceedings.

### **B) Confidentiality of the reported person, witnesses and all third parties mentioned in the Report**

#### **Confidentiality**

All persons involved are entitled to confidentiality in order to avoid unnecessary damage to their privacy and reputation. Therefore, the identity of the reported person, the facts reported, and the subsequent investigation and findings are kept confidential and limited to the strict necessity of the management of the Breach (subject to obligations arising from the law or the applicable legal proceedings).

Information shared must be kept confidential at any circumstances (regardless of the job position or seniority in Haleon Hungary) and, if necessary for the investigation to inform another person, the Case Manager should be consulted and approve. An unauthorized disclosure may lead to disciplinary actions.

#### **Privacy**

Haleon Hungary processes the data of the persons concerned by the Report in line with the provisions of the Hungarian Whistleblowing Act, the EU Regulation 679/2016 ("GDPR") and relevant Hungarian laws, and the Data Privacy Notice of Haleon Hungary.



## 5.8 Ireland

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Ireland by any legal entities with an excess of 50 employees ("**Haleon Ireland**").

This section applies to Haleon Ireland employees (whether employed on a permanent, temporary, full-time, part-time or fixed-term basis) and persons who have acquired information about the Breaches (as defined below) in the context of a working or professional relationship or provide services to Haleon Ireland. These persons include independent contractors, sub-contractors, service providers, suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, agency staff, persons on work experience, ex-employees, volunteers and trainees.

This section also applies to those who report a breach of which they became aware during a recruitment process or pre-contractual negotiations (collectively "**Reporters**")

### **What concerns do this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers the reporting of complaints and concerns (collectively, "**Reports**") relating to the following matters:

- criminal offences that have been, are being or are likely to be committed;
- a failure or likely failure to comply with any legal obligation, other than one arising under a contract of employment or a contract to provide services personally;
- a miscarriage of justice that has occurred, is occurring or is likely to occur;
- the actual or likely endangerment of the health or safety of any individual;
- damage or likely damage to the environment;
- an unlawful or otherwise improper use (or likely improper use) of funds or resources of a public body or other public money;

- an act or omission by or on behalf of a public body that is oppressive, discriminatory or grossly negligent or which constitutes gross mismanagement; and
- information tending to show that any of the preceding matters has been, is being or is likely to be concealed or destroyed or that an attempt has been, is being or is likely to be made to conceal or destroy such information.

(together, the "**Breaches**").

This section does not cover Reports relating to the Reporter's own personal circumstances, grievances, complaints or employment relationship. Such concerns will generally fall outside the scope of this section and it may be more appropriate to raise such matters under a different Haleon Ireland policy or procedure.

### **How to internally report a Breach or concerns covered by this section locally**

In Ireland, Reporters may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources. If you wish to have the concern heard and where appropriate investigated locally, please email [Haleon.SpeakUp.Ireland@Haleon.com](mailto:Haleon.SpeakUp.Ireland@Haleon.com) with your concern.

### **Investigation process and feedback**

Once a Report has been received, Haleon Ireland will carry out an initial assessment to determine whether there is *prima facie* evidence of a Breach and, if so, appropriate action will be taken which may include an investigation. The Reporter may be asked to provide further information in connection with any such investigation process.

Haleon Ireland will aim to keep the Reporter informed of the progress of any investigation and its likely timescale. However, sometimes the need for confidentiality may prevent us from giving the Reporter specific details of the investigation or any action taken as a result. The Reporter is required to treat any information about the investigation as strictly confidential.

Fair and due process requires that any person accused of wrongdoing or a Breach should be made aware of, and given the opportunity to respond to, any allegations made against them.

If the Reporter's identity is known, they will be provided with feedback within three months of acknowledgment of receipt of the Report. Furthermore, if the Reporter so requests in writing, they will be provided with further feedback at intervals of 3 months until such time as the procedure relating to the Report is closed.

## **Anonymity and Confidentiality**

Reports may be made anonymously or on an open basis. However, we strongly encourage Reports to be made on an open basis, where possible. Anonymous reporting may limit the extent to which we are able to fully investigate Reports and take remedial action.

Haleon Ireland will take steps to maintain confidentiality for all parties involved, to the extent reasonable and practicable under the circumstances.

Haleon Ireland will not, without the Reporter's explicit consent, disclose their identity or any information from which their identity may be directly or indirectly deduced, to another person, other than those (including members of staff designated under legislation) whom Haleon Ireland reasonably considers may be necessary for the purposes of the receipt or transmission of, or follow-up on, Reports as required under legislation.

The prohibition on disclosure will not apply where:

- the disclosure is a necessary and proportionate legal obligation in the context of investigations or judicial proceedings;
- the person to whom the Report was made or transmitted:
  - shows that they took all reasonable steps to avoid disclosing the Reporter's identity or any information from which it could be deduced, or
  - reasonably believes that disclosing their identity or any such information is necessary for the prevention of serious risk to the security of the State, public health, public safety or the environment;
- the disclosure is otherwise required by law.

Where the Reporter's identity or any other information from which their identity may be directly or indirectly deduced is disclosed to another person, the Reporter will be notified in writing in advance, together with the reasons for the disclosure unless this would jeopardise:

- the effective investigation of the wrongdoing;
- the prevention of serious risk to the security of the State, public health, public safety or the environment; or
- the prevention of crime or the prosecution of a criminal offence.

Retaliation against Reporters, whether direct or indirect, and persons who facilitate or otherwise assist in the making of the Report or the investigation process will not be tolerated.

## **Malicious or False Reports**

If it is found that a person knowingly reported false information or that a Report of wrongdoing was made maliciously, the person who made the Report may be subject to disciplinary action.

## **External Reporting locally**

Haleon Ireland strongly encourages Reports to be made internally so that any concerns can be resolved. However, should Reporters decide to Report their concerns externally, the prescribed persons are set out in the Protected Disclosures Act 2014 (Disclosure to Prescribed Persons) Order 2020 (SI 367/2020), available [here](#). The Reporter may also make a Report to the Office of the Protected Disclosures Commissioner or, where relevant, to institutions, bodies offices or agencies of the European Union.

A Reporter may make a Report to a prescribed person if the person reasonably believes that the Breach is within the remit of the prescribed person and the information the person discloses and any allegation in it are substantially true.

## **Records**

Haleon Ireland will keep a record of all Reports made in accordance with this section. Records will be retained for no longer than is necessary and proportionate for Haleon Ireland to comply with its legal obligations.

## **5.9 Italy**

[TO BE UPDATED]

## 5.10 Netherlands

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in the Netherlands by local legal entities with 50+ employees ("**Haleon NL**").

This section applies to Haleon NL employees, but we also accept Reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon NL or any other Haleon legal entity. The categories of person who may make Reports by virtue of their working or professional relationship, in addition to employees of Haleon NL, include independent contractors, agency workers, job candidates, sub-contractors, service providers, suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, members of the administrative, management or supervisory body, and suppliers and anyone working under the supervision of them) who reports a (suspected) misconduct or (suspected) abuse, volunteers and trainees (collectively, "**Reporters**").

### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters, relating to an act or omission involving the public interest concerning the following issues:

- the violation or risk of violation of a statutory regulation or internal rules containing a concrete obligation and established by an employer pursuant to a statutory regulation; or
- the danger to public health, to the safety of persons, to damage to the environment or to the proper functioning of the company by improper acts or omissions.

The public interest is at stake in any case if the act or omission does not only affect personal interests, but must also have either a pattern or structural character or the act or omission must be severe or extensive.

### **How to internally report a breach or concerns covered by this section locally**

In the Netherlands, Reporters may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and where appropriate investigated locally, please reach out to the local officer for the Netherlands ("**Local Officer**") to file a Report and who will follow up on the Report with due care. You can reach out to Michaël Falcomer (HR Business Partner Benelux) via email: [haleon.speakup.netherlands@Haleon.com](mailto:haleon.speakup.netherlands@Haleon.com) or by phone on +32 475 824 320 or to Marie-Maud Danmanville (Legal & Compliance Director France & Benelux) via email: [haleon.speakup.netherlands@Haleon.com](mailto:haleon.speakup.netherlands@Haleon.com) or by phone on +33 6 82 82 70 95 with your concern.

You may report your concerns in writing, orally by telephone or request a face-to-face meeting with the Local Officer.

Haleon may request the assistance of an external law firm ("**Law Firm**") to obtain advice as to how to proceed in accordance with local legislation.

### **External reporting locally**

Haleon NL strongly encourages Reports to be made internally so that any concerns can be resolved. However, should Reporters decide to report their concerns externally, the competent authorities in the Netherlands are set out below:

- Authority for Consumers and Markets (*Autoriteit Consument en Markt*) (<https://www.acm.nl>)
- Authority for Financial Markets (*Autoriteit Financiële Markten*) ([www.afm.nl](http://www.afm.nl))
- Data Protection Authority (*Autoriteit persoonsgegevens*) ([www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl))
- De Nederlandsche Bank N.V. ([www.dnb.nl](http://www.dnb.nl))
- Dutch Whistleblowers Authority (*Huis voor Klokkeluiders*) ([www.huisvoorklokkeluiders.nl](http://www.huisvoorklokkeluiders.nl))
- Health and Youth Care Inspectorate (*Inspectie gezondheidszorg en jeugd*) ([www.igj.nl](http://www.igj.nl))
- Dutch Healthcare Authority (*Nederlandse Zorgautoriteit*) ([www.nza.nl](http://www.nza.nl))
- Authority for Nuclear Safety and Radiation Protection (*Autoriteit Nucleaire Veiligheid en Stralingsbescherming*) ([www.autoriteitnvs.nl](http://www.autoriteitnvs.nl))
- Other authorities appointed by the minister or statute

Information on how to report can be found on the respective authority's website. It is also possible to seek advice on a confidential basis from the Advice Department of the Dutch Whistleblowers Authority before reporting any breaches (E: [advies@huisvoorklokkeluiders.nl](mailto:advies@huisvoorklokkeluiders.nl)).

## **What to expect when reporting locally**

- All Reports received through the local reporting channel are directly managed by the Local Officer and the Law Firm. Once a Report is received the Local Officer will assess whether the Report falls within the scope of this section or the Policy and whether it should result in further investigation pursuant to either the Policy or this section. The Reporter will be informed accordingly.
- All Reports received through other means (i.e. by HR business partners) will be sent promptly by the recipients to the Local Officer and the Law Firm using the local reporting channel and will be kept confidential.
- The Reporter will receive feedback on the progress of the investigation, within a reasonable timeframe not exceeding three (3) months from the acknowledgement of receipt.
- Retaliation against a Reporter, whether direct or indirect, will not be tolerated. This protection against retaliation provided by the Dutch Act, also extends to:
  - Facilitators who advise a Reporter in the reporting process in a work-related context and whose advice is confidential;
  - a third party who is connected with a Reporter and who could suffer a detriment at the hands of Haleon NL or a person or organisation with which the Reporter is otherwise connected in a work-related context
  - a legal entity that the Reporter owns, works for or is otherwise connected with in a work-related context; and
  - the Local Officer(s) to whom Reports can be reported and who will follow up on the Report.



## 5.11 Poland

This country section for Poland (the "**Section**") is set out in accordance with the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws No. 2024, item 928.) ("**Whistleblower Protection Act**"). It supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (collectively the "**Policy**"). In the event of a conflict, this Section shall prevail.

### Who this Section applies to locally

This Section applies in Poland in Haleon legal entities hiring at least 50 persons (collectively "**Haleon Poland**").

This Section applies to Haleon Poland current or former employees (whether employed on a permanent, temporary, full-time, part-time or fixed-term basis) and other persons who have acquired information about the Breaches (as defined below) in a work-related context (working or professional relationship with or providing services to Haleon Poland). These persons include current or former independent contractors, sub-contractors, service providers, suppliers, members of management, auditing or supervisory corporate bodies and commercial proxies, shareholders, agency staff, persons on work experience, volunteers, interns, trainees, and persons working under the supervision of contractors, suppliers, service providers and their sub-contractors, including based on a civil law contract. This Section also applies to those who report a breach of which they became aware during a recruitment process or pre-contractual negotiations (collectively "**Reporters**").

### What concerns does this Section apply to locally

This Section covers the reporting of complaints and concerns (collectively "**Reports**") relating to action or failure to act, in breach of law or with aim to circumvent the law, relating to (a) corruption, (b) public procurement; (c) financial services, products and markets; (d) prevention of money laundering and terrorist financing; (e) product safety and compliance; (f) transport safety; (g) protection of the environment; (h) radiation protection and nuclear safety; (i) food and feed safety, (j) animal health and welfare; (k) public health; (l) consumer protection; (m) protection of privacy and personal data; (n) security of network and information systems; (o) financial interests of the State Treasury of Poland, any local self-government unit or European Union; (p) internal market of the European Union, including public law competition and state aid rules, as well as corporate taxation; (r) constitutional freedoms and rights of the human being and the citizen occurring in the relations of the individual with public authorities (collectively "**Breaches**").

This Section only covers Reports with respect to which (a) the Reporter has revealed their identity to Haleon Poland, and (b) the Reporter had reasonable grounds to believe that information contained in the Report: (i) is true at the time Report is being made, and (ii) informs on a violation of law within the scope of Breaches indicated above.

This Section does not cover anonymous reports and reports relating to individual employee grievances, complaints relating to job performance, or complaints related to the terms and conditions of employment (unless they fall within the scope of Breaches indicated above). Such concerns will generally fall outside the scope of this Section and it may be more appropriate to raise such matters under a different Haleon Poland policy or procedure.

### **How to internally report a Breach or concerns covered by this Section locally**

In Poland, Reporters may use the reporting channels identified in the End-to-End Concerns Policy to report concerns under the End-to-End Concerns Policy. However, using these channels means the concern will be received and potentially investigated using group resources in accordance with the End-to-End Concerns Policy, so this Section and the Whistleblower Protection Act will not apply.

If you wish to have the report of a Breach received and where appropriate investigated locally under this Section and in accordance with the Whistleblower Protection Act, please use one of the local reporting channels indicated in this Section, that is:

- a) email the local Investigations Unit at: [[Whistleblower.Poland@Haleon.com](mailto:Whistleblower.Poland@Haleon.com)], or
- b) if you would like to make a Report in person, please contact any member of the local Investigations Unit at: [[Whistleblower.Poland@Haleon.com](mailto:Whistleblower.Poland@Haleon.com)] or at their company email address (using private mode). A meeting will be arranged as soon as possible, and no later than within 14 days from the time we receive your request.

The receipt of the Report under this Schedule will be acknowledged within 7 (seven) days of receipt, unless the Reporter failed to provide address for service or email address where such acknowledgment can be delivered.

Reports submitted through local reporting channels under this Schedule will be received, managed and (if prerequisites are met) followed-up on by the local Investigations Unit, which is authorized by Haleon Poland receive and follow up on Reports made under this Schedule.

The local Investigations Unit comprises of from 1 (one) to 3 (three) members who are appointed by Haleon Poland's Management Board. Currently the only member of the local Investigations Unit is: Mr Marcin Jaworski (Marcin.Jaworski@Haleon.com). Members of the Local Investigation Unit may change over time. The current composition of the local Investigations Unit is available on the Haleon Poland's intranet portal.

Haleon Poland may request the assistance of further experts or external advisors to proceed in a thorough and compliant way.

### **Investigation process and feedback**

Once a Report has been received under this Schedule, the local Investigations Unit will carry out an initial assessment to determine whether there is *prima facie* evidence of a Breach and, if so, appropriate action will be taken which may include an investigation. All follow-up actions will be performed with due diligence. The Reporter may be asked to provide further information in connection with any such investigation process.

Haleon Poland will aim to keep the Reporter informed of the progress of any investigation and its likely timescale. However, sometimes the need for confidentiality may prevent us from giving the Reporter specific additional details of the investigation or details of actions taken as a result. Haleon Poland will, each time, provide feedback on the actions planned or taken in relation to the Report, and reasons for such actions, within 3 (three) months of acknowledgment of receipt of the Report or of the deadline for acknowledging the receipt (if acknowledgment has not been provided). The Reporter is required to treat any information about the investigation as strictly confidential.

### **Anonymity and confidentiality**

Haleon Poland will take steps to maintain confidentiality for all parties involved, to the extent required by law under the circumstances. Haleon Poland will not, without the Reporter's explicit consent, disclose their identity or any information from which their identity may be directly or indirectly deduced, to any unauthorized person.

The prohibition on disclosure will not apply where:

- a) the disclosure is a necessary and proportionate legal obligation in the context of public body investigations or judicial proceedings, including to ensure right of defense of the person concerned; or
- b) the disclosure is otherwise required by law.

Retaliation against those making Reports, whether direct or indirect, and persons who facilitate or otherwise assist in the making of the

Report or the investigation process will not be tolerated. Haleon Poland recognizes all forms of retaliation set out in the Whistleblower Protection Act.

### **Malicious or false Reports**

If it is found that a person knowingly reported false information, the Reporter may be subject to disciplinary action.

### **External reporting locally**

Haleon Poland encourages Reports to be made internally so that any concerns can be resolved. However, the Reporter may submit a Report to external reporting channels, which include: superior and central government administration bodies, local government administration bodies, and other state bodies, mayor, starost, marshal, regional accounting chambers, or to institutions, bodies offices or agencies of the European Union, as relevant to their scope of competence. Whenever the Reporter is unable to identify the relevant body, Reports can be made to the Commissioner for Human Rights (Ombudsman).

### **Records**

Haleon Poland will keep a record of all Reports made in accordance with this Section. Records will be retained for 3 years following the end of the calendar year in which follow-up actions, or proceedings initiated as a result of such follow-up actions, have been completed.

## 5.12 Portugal

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Portugal by local legal entities with 50+ employees ("**Haleon Portugal**").

This section applies to Haleon Portugal employees, but we also accept reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Portugal or any other Haleon legal entity. The categories of person who may make reports by virtue of their working or professional relationship, in addition to employees of Haleon Portugal, include independent contractors, sub-contractors, service providers, suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, volunteers and trainees (collectively "**Reporters**").

### **What concerns do this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters relating to the following matters:

- Violent crime, especially violent and highly organised crime, as well as organised and economic-financial crime
- In the field of national defence and security, any act or omission contrary to the procurement rules contained in the European Union acts referred to in part i.A of the Annex to Directive (EU) 2019/1937, or contrary to the purposes of those rules.

### **How to internally report a breach or concerns covered by this section locally**

In Portugal, Reporters may use the reporting channels identified in the End-to-End Concerns Policy and the Code of Conduct. However, using this channel means the concern will be heard and potentially investigated using group resources. If you wish to have the concern heard and where appropriate investigated locally, please email [Haleon.SpeakUp.Portugal@Haleon.com](mailto:Haleon.SpeakUp.Portugal@Haleon.com) with your concern.

## **External reporting locally**

Haleon Portugal strongly encourages Reports to be made internally so that any concerns can be resolved. However, should Reporters decide to report their concerns externally, the competent authorities are set out below:

- the Public Prosecutor's Office;
- the criminal police agencies;
- the Bank of Portugal;
- the independent administrative authorities;
- public institutes;
- inspectorates-general and similar entities and other central services of the direct administration of the State endowed with administrative autonomy;
- local authorities; and
- public associations.

## 5.13 Romania

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Romania by local legal entities with 50+ employees ("**Haleon Romania**").

This section applies to Haleon Romania employees, but we also accept Reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Romania, as described below. The categories of person who may make Reports by virtue of their working or professional relationship, in addition to current or former employees of Haleon Romania, include:

- Independent contractors, sub-contractors, service providers, suppliers, who performed work or provided services for or to Haleon Romania;
- Shareholders, members of the board, members of management, auditing or supervisory corporate bodies, including non-executive members of the board of directors;
- Volunteers and trainees;
- Any persons working under the supervision and direction of contractors, subcontractors and suppliers who performed work or provided services for or to Haleon Romania;
- Job candidates in relation to a recruitment process at Haleon Romania, who obtained information in relation to their concern during the recruitment process or other pre-contractual negotiations;
- Potential service providers to Haleon Romania, such as manufacturers, suppliers, contractors, or consultants, who obtained information in relation to their concern during the pre-contractual negotiations; and
- Persons who anonymously Report or publicly disclose information regarding violations of the law.

(collectively, "**Reporters**").

### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters relating to the following matters:

- Breaches falling within the scope of the Romanian laws and European Union acts set out in the Annex 2 to the Romanian Whistleblowing Law (i.e., Law No. 361/2022 on the protection of whistleblowers in the public interest) that concern the following areas: (a) public procurement, (b) financial services, products and markets, and prevention of money laundering and terrorist financing, (c) product safety and compliance, (d) transport safety, (e) protection of the environment, (f) radiation protection and nuclear safety, (g) food and feed safety, animal health and welfare, (h) public health, (i) consumer protection, (j) protection of privacy and personal data, and security of network and information systems.
- Breaches related to the internal market, as referred to in Article 26(2) of the TFEU, including breaches of the European Union rules on competition and State aid, as well as breaches related to the internal market in terms of acts that violate the rules on corporate taxation or mechanisms whose purpose is to obtain a fiscal advantage that contravenes the object or purpose of the law applicable to corporate taxation, which represent disciplinary misconducts, contraventions or crimes, or which are contrary to the object or purpose of the law.

### **How to internally report a breach or concerns covered by this section locally**

In Romania, the Reporters may report a breach or concerns covered by this section using the reporting channels identified in the End-to-End Concerns Policy.

Reports made under this section shall be investigated by the Haleon group response team, respectively by Incident Classification Group ("**ICG**"), which is comprised of the Security, Investigations and Resilience team, HR and Legal, with other stakeholders such as Forensics, Tech and Compliance brought in where necessary to advise on specific concerns.

Haleon Romania may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.

### **What a Report should contain**

According to the Romanian Whistleblowing Law, a Report should include, at least, the following:

- the name and the contact details of the Reporter;
- the workplace-related context in which the information was obtained;
- the person concerned, if known;
- the description of the fact likely to constitute a violation of the law within the Company and, as appropriate;



- the evidence in support of the Report; and
- the date and signature if the case.

If the Report does not contain the above-mentioned elements, other than the Reporter's identification data, the Reporter may be asked to provide additional information within fifteen (15) days. If the Reporter fails to provide the requested information within the foregoing timeframe, the respective Report will be closed without further due.

### **Anonymous reporting**

Anonymous Reports will be analysed to the extent they contain indications of the alleged breach of the law.

If the anonymous Report does not contain enough information about violations of the law to allow analysis and resolution of respective Report, the Reporter may be asked complete it within fifteen (15) days. If the Reporter fails to provide the requested information within the foregoing timeframe, the anonymous Report will be closed without further actions taken in relation to such Report.

### **Record keeping**

The Reports are stored for a period of five (5) years, as provided under the Romanian Whistleblowing Law. On expiry of this period, Reports will be destroyed.

### **External reporting locally**

Haleon Romania strongly encourages Reports to be made internally so that any concerns can be resolved. However, the Reporter may submit a Report to external reporting channels. The National Agency for Integrity is the authority with general competencies in relation to external whistleblowing reporting.

Further information on how you can report a concern can be found on the website of the National Agency for Integrity, respectively on: Informații generale – Avertizori în interes public ([integritate.eu](http://integritate.eu))

### **Other aspects**

If the Reporter is subject to a disciplinary proceeding due to making a Report (whether through internal or external reporting channels, or public disclosure), the relevant disciplinary committee or similar body within Haleon Romania shall, on Reporter's prior request, invite the media, a representative of the union or professional association, or a representative of the employees, as the case may be.

## 5.14 Slovakia

his country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Slovakia by **Haleon Levice, s.r.o.**, having its registered office at Priemyselný park Géňa, Ul. E. Sachsa 4-6, 934 01 Levice, Identification No.: 47 249 153 ("**Haleon Levice**").

This section applies to Haleon Levice employees, but we also accept reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Levice or any other Haleon legal entity. The categories of persons who may make reports by virtue of their working or professional relationship, in addition to employees of Haleon Levice, include:

- Independent contractors;
- Individuals exercising rights associated with the participation in a legal entity;
- Members of a body of a legal entity;
- Individuals performing tasks within the scope of the activity of a legal entity, in its interest, on its behalf or on its account;
- Volunteers;
- Interns;
- Individuals performing rights and obligations arising from the contract, the subject of which is the provision of supplies, services, construction works or other similar performance

(collectively "**Reporters**").

### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters relating to:

- specific criminal acts as well as all criminal acts, for which the Slovak Criminal Code sets out a prison sentence with the upper limit over two years,
- administrative offence for which the maximum fine is to be calculated based on a formula; and
- administrative offence for which the maximum fine exceeds €30,000.

## **How to internally report a breach or concerns covered by this section locally**

In Slovakia, employees may use the reporting channels identified in the End-to-End Concerns Policy and the Code of Conduct. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you wish to have the concern heard and where appropriate investigated locally, please email [OznamenieLevice@Haleon.com](mailto:OznamenieLevice@Haleon.com) with your concern. Please note that any concerns regarding Reports that Reporters wish to report in Slovakia may be reported locally, orally or in writing, also during a physical meeting.

### **Investigation process**

If a Reporter submits a Report using the local channels identified in this section, the person responsible for the local channel will carry out an assessment to determine the scope of any investigation. Where the Report can be handled at local level and it relates to purely local circumstances even in terms of its consequences, the Report will be handled at local level with the support of the local HR Department or his/her designee.

During the investigation process it is possible that the team in charge of the investigation could request additional information from the Reporter. The person responsible for the investigation, as well as their team, shall maintain communication with the Reporter and will provide feedback no later than 90 days from the date of the notice of receipt. The persons or services involved in the investigation process have, by virtue of their position or status, the competence, authority and means necessary to carry out their role. Alternatively, local HR Department may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation or may involve other forensic third-party providers to assist with an investigation if required, who will be under confidentiality obligations.

The Reporter's identity and information from which his/her identity can be directly or indirectly traced will not be disclosed without his/her consent. Reports will be shared with the local HR Department, or their designee, in compliance with applicable information-sharing provisions.

### **Designated person**

The designated person is the following individual engaged by Haleon Levice or the following department at Haleon Levice: local HR Department.

## **External reporting locally**

Haleon Levice strongly encourages Reports to be made internally so that any concerns can be resolved. However, should Reporters decide to submit their Reports externally, the competent authority is the Office for Protection of Whistleblowers (*Úrad na ochranu oznamovateľov*, <https://www.oznamovatelia.sk/>).

## **Protection**

If applicable, the Reporter may apply for protection in:

- criminal proceedings to the public prosecutor;
- administrative-offence proceedings to the respective public authority in charge of the proceedings;
- relation to any legal action affecting the employment relationship to the Office for Protection of Whistleblowers.

Haleon Levice may not take any Retaliation against the Reporter for submission of the Report.

## **Record keeping**

Haleon Levice must maintain records about Reports filed by the Reporters for a period of three years from the date of receipt of the Report.

Haleon Levice is obliged to keep evidence of the Reports received, covering the following scope:

- date of filing;
- Reporter's name, surname and address, save for a case of anonymous Reporter;
- the subject of the Report;
- results of the investigation; and
- date of closing of the investigation.

## **Data privacy**

Haleon Levice will be the data controller of the personal data processed for the purpose of managing the whistleblowing system and investigating the Reports, according to its obligation to comply with legal provisions regarding the implementation of a whistleblowing system.

Haleon Levice may process personal data of the Reporters and the persons who are the subject of the Reports. In particular, the following categories

of personal data may be collected and processed as part of the investigation of Reports:

- Identity, functions and contact details of the Reporter;
- Identity, functions and contact details of the persons who are the subject of the Report;
- Identity, functions and contact details of persons involved in the collection or processing of the Report;
- Facts reported;
- Elements collected within the framework of the verification of the reported facts;
- Investigation reports; and
- Follow-up to the Report.

Personal data will only be accessed by the local designated person, although they may allow access to the Head of HR for taking disciplinary measures, to the Head of Legal for taking legal action, to the data protection officer, to any third party where necessary for taking corrective measures, and to data processors that may assist with the investigations (which may include but it is not limited to HR and legal teams and third party providers).

Furthermore, the local designated person may transfer personal data to public authorities, courts or the Public Prosecutor Office in order to comply with legal obligations or to bring or defend Haleon Levice from claims and liabilities arisen from the facts mentioned in the Report or gathered as part of the investigation. If the Reporter's personal data is transferred to those authorities, Haleon Levice will inform the Reporter in advance, unless that may risk an investigation or legal proceedings or contravene applicable regulations from time to time.

As part of the Policy, personal data acquired by Haleon Levice may be transferred outside of the European Economic Area. To provide an adequate level of data protection for the transfer of personal data through the whistleblowing system, Haleon Levice has entered into an agreement including the European Commission's standard contractual clauses with the relevant entities of the Haleon group, which may act as data processors for the purpose of providing the underlying technology that supports the whistleblowing system. Data subjects can obtain a copy of such standard contractual clauses by sending an e-mail to [IRM.Support@haleon.com](mailto:IRM.Support@haleon.com)

Personal data will be retained as described in section "Record keeping" above.

Data subjects may exercise their rights of access, rectification, erasure, objection, limitation of processing and portability of their data, where applicable under the applicable regulations, by sending an email to [IRM.Support@haleon.com](mailto:IRM.Support@haleon.com)

In addition, they may also lodge a complaint with the relevant supervisory authority: the Slovak Data Protection Authority (*Úrad na ochranu osobných údajov Slovenskej republiky*, <https://dataprotection.gov.sk/uouu/>). However, in the event that the persons who are the subject of the Reports exercise their right to object, it shall be presumed that there are compelling legitimate grounds for processing his or her personal data, unless there is evidence to the contrary.

## 5.15 Spain

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### Who this section applies to locally

This policy is implemented in Spain by

- Haleon Spain, S.A.U.; and
- Haleon Alcala, S.A.U.

together ("**Haleon Spain**").

This section applies to Haleon Spain employees but we also accept reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Spain or any other Haleon legal entity. The categories of person who may make reports by virtue of their working or professional relationship, in addition to employees of Haleon Spain, include independent contractors, any person working under the supervision and direction of contractors, sub-contractors service providers or suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, volunteers and trainees, former employees or candidates (collectively "**Reporters**").

### What concerns does this section apply to locally

In addition to the topics that are set out in the Policy, this section covers complaints and concerns (collectively, "**Reports**") of employees, shareholders and others, employed or engaged by Haleon Spain relating to acts or omissions that may constitute a "serious" or "very serious" criminal offence or administrative infringement, including all those serious

or very serious criminal offences or administrative infringements that involve economic loss for the Public Treasury and for Social Security.

### **How to internally report a breach or concerns covered by this section locally**

In Spain, employees may use the reporting channels identified in the End-to-End Concerns Policy and the Code of Conduct. However, using this channel means the concern will be heard and potentially investigated using group resources.

Any concerns regarding Reports that Reporters wish to report locally in Spain may also be reported, in writing, to: [Haleon.SpeakUp.Spain@Haleon.com](mailto:Haleon.SpeakUp.Spain@Haleon.com)

Reports made through this channel will be received by Gueorgui Roussev, who is authorized by Haleon Spain to receive and follow up on Reports received through this channel (the "**Local Reporting System Manager**").

If your Report concerns the Local Reporting System Manager, you can directly send your Report to any member of the Board of Directors of your employing entity or through the group channels identified in the End-to-End Concerns Policy and the Code of Conduct.

Likewise, if a Report is not received through the reporting channels mentioned in this Policy but through other unofficial channels or employees, the employee receiving such Report must immediately communicate the same to the Local Reporting System Manager within a maximum period of 48 hours, immediately deleting the Report received. The person who has received the Report must keep the Report strictly confidential. Failure to comply with these reporting and confidentiality obligations may lead to disciplinary action.

Reports may be made anonymously or on an open basis. However, we strongly encourage Reports to be made on an open basis, where possible. Anonymous reporting may limit the extent to which we are able to fully investigate Reports and take remedial action.

A Report made on an anonymous basis will be investigated, provided that the seriousness of the alleged facts is evidenced and the factual elements supporting the claim are sufficiently detailed.

### **Investigation process**

If you make a Report using the local channels identified in this Spain section, the Local Reporting System Manager, or their designee, will carry out an assessment to determine the scope of any investigation to elect the investigation team that will handle the investigation process depending on the nature of the Report, including HR and legal teams.

The Report may be shared with those individuals handling the investigation, always guaranteeing the confidentiality of the Report. If the Local Reporting System Manager, or their designee, considers that the scope of the Report made does not allow local investigation (i.e. if it cannot or can no longer be handled at the local level and/or its consequences exceed the local level), the Report may be shared with the General Counsel, or his designee, who may ask the Reporter to provide further information in connection with the investigation process. The persons or services involved in the investigation process have, by virtue of their position or status, the competence, authority and means necessary to carry out their role. Alternatively, the Local Reporting System Manager may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation or may involve other forensic third-party providers to assist with an investigation if required, who will be under confidentiality obligations.

During the investigation process it is possible that the team in charge of the investigation could request additional information from the Reporter. Additionally, if there is any other person affected by the Report, the affected person will be informed of the actions or omissions attributed to him/her and will be entitled to be heard at any time, but will not be informed of the identity of the Reporter.

The investigation process will be completed under a presumption of innocence and respecting the honour of the persons concerned.

The maximum length of the investigation proceeding would be three (3) months, except in cases of special complexity that require an extension of the term, in which case, this may be extended up to a maximum of three (3) additional months. The Reporter will be provided with feedback on the action envisaged or taken as follow-up to the Report, as far as it is possible, and subject to the Company's other obligations, including applicable laws and internal policies.

## **Confidentiality**

Consistent with the End-to-End Concerns Policy, all investigations will be conducted in a confidential manner, so that information will be disclosed only as needed to facilitate review of the investigation materials or otherwise as required by law.

The Local Reporting System Manager will retain on a strictly confidential basis, as required under the Company's record retention policy and applicable regulations in effect from time to time, all records relating to any Report and to the investigation and resolution thereof.

We guarantee the confidentiality even when the communication is sent to non-competent personnel, who will have been trained in this matter and warned of the classification of its violation as a "very serious"



offence. There is also an obligation to everyone who receives a Report by mistake to send it to the Local Reporting System Manager.

## **Record keeping**

Reports will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the whistleblowers, the subjects of the Report and any third parties mentioned in the Report, as well as to preserve the Company's defence right, taking into account the time required for any further investigations.

In particular, personal data relating to out-of-scope Reports, special categories of personal data (except where necessary due to the nature of the Report), untruthful information, and personal data that is unnecessary for the investigation will be destroyed without delay.

If no investigation is initiated within three (3) months after receipt of an in-scope Report, personal data relating to this Report will be destroyed, unless duly anonymized.

If no action is taken following an in-scope Report, the personal data relating to this Report will be destroyed by Haleon Spain once the investigation is finished and the decision not to take any further action is made.

In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will be retained until the end of the proceedings or the end of the limitation period for appeals against the decision and maximum for ten (10) years, unless it is necessary to keep the data for a longer period of time to preserve the Company's defence right.

## **Data privacy**

The management body of each entity that is part of Haleon Spain will be the data controller of the personal data processed for the purpose of managing the whistleblowing system and investigating the Reports, according to its obligation to comply with legal provisions regarding the implementation of a whistleblowing system pursuant to Law 2/2023.

Haleon Spain may process personal data of the whistleblowers and the persons who are the subject of the Reports. In particular, the following categories of personal data may be collected and processed as part of the investigation of Reports:

- Identity, functions and contact details of the whistleblower;
- Identity, functions and contact details of the persons who are the subject of the Report;

- Identity, functions and contact details of persons involved in the collection or processing of the Report;
- Facts reported;
- Elements collected within the framework of the verification of the reported facts;
- Investigation reports; and
- Follow-up to the Report.

Personal data will only be accessed by the Local Reporting System Managers, although they may allow access to the Head of HR for taking disciplinary measures, to the data protection officer, to any third party where necessary for taking corrective measures, and to data processors that may assist with the investigations (which may include but it is not limited to HR team and third party providers).

Furthermore, the Local Report System Managers may transfer personal data to public authorities, courts or the Public Prosecutor Office in order to comply with legal obligations or to bring or defend Haleon Spain from claims and liabilities arisen from the facts mentioned in the Report or gathered as part of the investigation. If whistleblower's personal data is transferred to those authorities, Haleon Spain will inform the whistleblower in advance, unless that may risk an investigation or legal proceedings or contravene applicable regulations from time to time.

As part of the policy, personal data acquired by Haleon Spain may be transferred outside of the European Economic Area. To provide an adequate level of data protection for the transfer of personal data through the whistleblowing system, Haleon Spain has entered into an agreement including the European Commission's standard contractual clauses with the relevant entities of the Haleon group, which may act as data processors for the purpose of providing the underlying technology that supports the whistleblowing system. Data subjects can obtain a copy of such standard contractual clauses by sending an e-mail to [privacy@haleon.com](mailto:privacy@haleon.com).

Personal data will be retained as described in section "Record Keeping" above.

Data subjects may exercise their rights of access, rectification, erasure, objection, limitation of processing and portability of their data, where applicable under the applicable regulations, by sending an email to [privacy@haleon.com](mailto:privacy@haleon.com). In addition, they may also lodge a complaint with the relevant supervisory authority: the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*). However, in the event that the persons who are the subject of the Reports exercise their right to object, it shall be presumed that there are compelling legitimate

grounds for processing his or her personal data, unless there is evidence to the contrary.

### **Protection against retaliation**

Individuals benefit from the protection provided by applicable Spanish statutory provisions. Specifically, the following individuals would be protected against retaliation:

- The whistleblower
- The legal representatives of employees in the exercise of their functions of advising and supporting the whistleblower
- Individuals who, within the organization in which the whistleblower works, assist the whistleblower in the process;
- Individuals who are related to the whistleblower and who may suffer reprisals, such as co-workers or relatives of the whistleblower,
- Individuals for whom the whistleblower works or with whom he/she has any other type of relationship in an employment context or in which he/she has a significant shareholding.

In particular, individuals are protected against any form of (threats and attempts of) retaliation (including termination, demotion, suspension, loss of benefits, threats, harassment or discrimination). Retaliation and reprisals by Haleon Spain or its employees against colleagues are a serious and material breach of this procedure.

Haleon Spain seeks to protect Individuals from retaliation and reprisals, and Haleon Spain will take appropriate disciplinary action against any employee who engages in retaliatory conduct. Conversely and for the avoidance of doubt, making a Report in bad faith could lead to disciplinary sanctions, up to and including dismissal.

When a Report or public disclosure has been made anonymously, the individual whose identity is subsequently revealed has the same protections as any individuals.

### **External reporting locally**

Haleon strongly encourages Reports to be made internally so that any concerns can be resolved and Haleon can take appropriate corrective measures. However, should employees decide to report their concerns externally, the competent authority is the Independent Authority for the Protection of Informants.

## 5.16 Sweden

This country section supplements the End-to-End Concerns Policy and the EU Whistleblowing Policy (the "**Policy**"). In the event of a conflict, this section shall prevail.

### **Who this section applies to locally**

This section is implemented in Sweden by local legal entities with 50+ employees ("**Haleon Sweden**").

This section applies to Haleon Sweden employees, but we also accept Reports from persons who have acquired information about the breaches outlined below in the context of a working or professional relationship with Haleon Sweden or any other Haleon legal entity. The categories of persons who may make Reports by virtue of their working or professional relationship, in addition to employees of Haleon Sweden, include job applicants, independent contractors, sub-contractors, service providers, suppliers, members of the board, members of management, auditing or supervisory corporate bodies, non-executives, volunteers and trainees, and other persons who perform work under the supervision and leadership of Haleon Sweden. The categories of persons who may make Reports also include persons who have previously been employed by Haleon Sweden or belonged to other categories listed above and acquired information about the breaches during their time with Haleon Sweden (collectively "**Reporters**").

### **What concerns does this section apply to locally**

In addition to the topics that are set out in this Policy, this section covers complaints and concerns (collectively, "**Reports**") of Reporters and relating to the following matters:

- Breaches of Swedish Law that implement or complete European Union Law;
- Breaches that counteract the purpose or aim of European Union Law; and
- Other complaints and concerns that are of such nature that it is in public interest that they are reported (Sw. *missförhållanden av allmänt intresse*).

### **How to internally report a breach or concerns covered by this section locally**

In Sweden, employees may use the reporting channels identified in the End-to-End Concerns Policy. However, using this channel means the concern will be heard and potentially investigated using group resources.

If you belong to another category of persons who may make Reports by virtue of working or professional relationship as defined above, or you are an employee and you wish to have the concern heard and where appropriate investigated locally, please email [Haleon.SpeakUp.Sweden@Haleon.com](mailto:Haleon.SpeakUp.Sweden@Haleon.com) or call +46708246483 and describe your concern. You may also request to report at a physical meeting which will be accommodated with a reasonable time period.

Haleon may request the assistance of an external law firm to obtain advice as to how to proceed in accordance with local legislation.

### **External reporting locally**

Haleon Sweden strongly encourages Reports to be made internally so that any concerns can be resolved. However, should Reporters decide to report their concerns externally, i.e., using a reporting channel maintained by a competent authority. The competent authorities are set out below:

- Arbetsmiljöverket (*The Swedish Work Environment Authority*) - [www.av.se](http://www.av.se)
- Boverket (*The Swedish National Board of Housing, Building and Planning*) - [www.boverket.se](http://www.boverket.se)
- Ekobrottsmyndigheten (*The Swedish Economic Crime Authority*) - [www.ekobrottsmyndigheten.se](http://www.ekobrottsmyndigheten.se)
- Elsäkerhetsverket (*The National Electrical Safety Board*) - [www.elsakerhetsverket.se](http://www.elsakerhetsverket.se)
- Fastighetsmäklarinspektionen (*The Swedish Estate Agents Inspectorate*) - [www.fmi.se](http://www.fmi.se)
- Finansinspektionen (*government authority tasked with monitoring the financial market*) - [www.fi.se](http://www.fi.se)
- Folkhälsomyndigheten (*Public Health Agency of Sweden*) - [www.folkhalsomyndigheten.se](http://www.folkhalsomyndigheten.se)
- Havs- och vattenmyndigheten (*Swedish Agency for Marine and Water Management*) - [www.havochvatten.se](http://www.havochvatten.se)
- Inspektionen för strategiska produkter (*Inspectorate of Strategic Products*) - [www.isp.se](http://www.isp.se)
- Inspektionen för vård och omsorg (*The Health and Social Care Inspectorate*) - [www.ivo.se](http://www.ivo.se)
- Integritetsskyddsmyndigheten (*The Swedish Authority for Privacy Protection*) - [www.imy.se](http://www.imy.se)

- Kemikalieinspektionen (*The Swedish Chemicals Agency*) - [www.kemi.se](http://www.kemi.se)
- Konkurrensverket (*The Swedish Competition Authority*) - [www.konkurrensverket.se](http://www.konkurrensverket.se)
- Konsumentverket (*The Swedish Consumer Agency*) - [www.konsumentverket.se](http://www.konsumentverket.se)
- Livsmedelsverket (*The Swedish Food Agency*) - [www.livsmedelsverket.se](http://www.livsmedelsverket.se)
- Läkemedelsverket (*The Swedish Medical Products Agency*) - [www.lakemedelsverket.se](http://www.lakemedelsverket.se)
- Länsstyrelserna (*County Administrative Boards*) - [www.lansstyrelsen.se](http://www.lansstyrelsen.se)
- Myndigheten för samhällsskydd och beredskap (*The Swedish Civil Contingencies Agency*) - [www.msb.se](http://www.msb.se)
- Naturvårdsverket (*The Swedish Environmental Protection Agency*) - [www.naturvardsverket.se](http://www.naturvardsverket.se)
- Post- och telestyrelsen (*The Swedish Post and Telecom Authority*) - [www.pts.se](http://www.pts.se)
- Regeringskansliet (*The Government Offices of Sweden*) - [www.regeringen.se](http://www.regeringen.se)
- Revisorsinspektionen (*The Swedish Inspectorate of Auditors*) - [www.revisorsinspektionen.se](http://www.revisorsinspektionen.se)
- Skatteverket (*The Swedish Tax Agency*) - [www.skatteverket.se](http://www.skatteverket.se)
- Skogsstyrelsen (*The Swedish Forest Agency*) - [www.skogsstyrelsen.se](http://www.skogsstyrelsen.se)
- Spelinspektionen (*The Swedish Gambling Authority*) - [www.spelinspektionen.se](http://www.spelinspektionen.se)
- Statens energimyndighet (*The Swedish Energy Agency*) - [www.energimyndigheten.se](http://www.energimyndigheten.se)
- Statens jordbruksverk (*The Swedish Board of Agriculture*) - [www.jordbruksverket.se](http://www.jordbruksverket.se)
- Styrelsen för ackreditering och teknisk kontroll (*The Board for Accreditation and Conformity Assessment, SWEDAC*) - [www.swedac.se](http://www.swedac.se)
- Transportstyrelsen (*The Swedish Transport Agency*) - [www.transportstyrelsen.se](http://www.transportstyrelsen.se)

## **Protection against retaliation under Swedish Whistleblowing Act**

Reporters who may make Reports by virtue of working or professional relationship as defined above under this section enjoy protection against retaliation under the Swedish Whistleblowing Act (Sw. *lag om skydd för personer som rapporterar om missförhållanden*, 2021:890) provided that the following conditions are met:

- The Reporter reported the complaint or concern using HALEON Sweden's local internal reporting line as described above, an external reporting line maintained by a competent authority or – subject to further conditions – by public disclosure;
- The Report relates to topics as set out in this section above;
- The Reporter had reasonable grounds to believe that the information about the complaint or concern was true at the time of reporting.

Under the Swedish Freedom of Press Act (Sw. *tryckfrihetsförordningen*) and the Swedish Fundamental Law on Freedom of Expression (Sw. *yttrandefrihetsgrundlagen*) everyone is free to communicate information on any subject whatsoever for the purpose of publication in programmes or technical recordings ("freedom to communicate information", Sw. *meddelarfrihet*) as well as right to procure information on any subject whatsoever in order to communicate or publish it ("freedom to procure information", Sw. *anskaffarfrihet*). An employee's duty of loyalty to HALEON Sweden as the employer may restrict these rights.

## 6 Translated Country Sections

### 6.1 Belgium

#### 1. Doel & toepassingsgebied

Deze Europese klokkenluiderspolicy (de "**Policy**") biedt informatie over de Europese Klokkenluidersrichtlijn en hoe werknemers in bepaalde omstandigheden ervoor kunnen kiezen om hun bezorgdheden lokaal te melden en, indien van toepassing, lokaal te laten onderzoeken, in plaats van op groepsniveau. Deze Policy is bedoeld als aanvulling op de End-to-End Processtandaard voor de Afhandeling van Bezorgdheden ("*End-to-End Concerns Management Process Standard*") (de "**End-to-End Policy voor Bezorgdheden**"). In geval van tegenstrijdigheid tussen de End-to-End Policy voor Bezorgdheden en deze Policy, zal deze Policy van toepassing zijn.

Er zijn landspecifieke addenda opgenomen in deze Policy, die aanvullende toelichting geven over hoe deze Policy in het betreffende land zal worden toegepast.

#### **Op welke bezorgdheden is deze Policy van toepassing in Europa?**

Deze Policy heeft specifiek betrekking op meldingen gedaan door werknemers, aandeelhouders en anderen die tewerkgesteld zijn door of werken voor een van de entiteiten die in de landspecifieke addenda worden genoemd en die verband houden met de volgende zaken ("**Meldingen**"):

- Inbreuken op het recht van de Europese Unie (een "**Inbreuk op het Unierecht**");
- De inbreuken die worden vermeld in de landspecifieke addenda; of
- Represailles tegen werknemers of rechtspersonen of natuurlijke personen die verbonden zijn met werknemers die Meldingen doen of het doen van Meldingen faciliteren met betrekking tot Inbreuken op het Unierecht.

Deze Policy is **niet** van toepassing op individuele personeelskwesties, klachten met betrekking tot de werkprestaties of klachten met betrekking tot de arbeidsvoorwaarden, die niet - naar hun aard - klachten zijn die betrekking hebben op een potentiële schending van integriteit, tenzij anders bepaald door de lokale regelgeving.

#### 2. Vereisten

##### 2.1 Een bezorgdheid melden



## **Intern melden met behulp van groepsmiddelen:**

Meldingen kunnen worden gedaan via de meldingskanalen die worden beschreven in de End-to-End Policy voor Bezorgdheden. Meldingen die via deze kanalen worden gedaan, worden ontvangen en verwerkt met behulp van groepsmiddelen (zijnde de Classificatiegroep voor Incidenten ("*Incident Classification Group*") ("*ICG*")). De ICG bestaat uit het Security, Investigations and Resilience team, HR en Legal, en waar nodig worden andere belanghebbenden zoals Forensics, Tech en Compliance ingeschakeld om advies te geven over specifieke bezorgdheden.

## **Lokaal intern melden:**

In aanvulling op de methodes die worden beschreven in de End-to-End Policy voor Bezorgdheden, kan een Melding worden gedaan via het e-mailadres dat wordt vermeld in de landspecifieke addenda, in overeenstemming met de lokale meldingsregelingen zoals uiteengezet in het relevante landspecifiek addendum.

## **2.2 Ontvangst van de Melding en het Onderzoek**

### **a) Een melding doen en de ontvangstbevestiging**

Meldingen kunnen worden gedaan via de kanalen die worden beschreven in de End-to-End Policy voor Bezorgdheden of via de methode die wordt beschreven in de bovenstaande paragraaf. Indien de Melder een Melding doet die binnen het toepassingsgebied van deze Policy of een relevant landspecifiek addendum valt, zal de Melder binnen zeven dagen na ontvangst van de Melding een ontvangstbevestiging krijgen. Indien de Melder om een fysieke ontmoeting verzoekt, zal deze binnen een redelijke termijn worden georganiseerd.

### **b) Het onderzoeksproces**

Zodra een Melding is ontvangen, kan de Melder worden verzocht om verdere informatie te verstrekken in verband met het onderzoeksproces.

Afhankelijk van de aard van de Melding kan het aangewezen zijn om de bezorgdheid te laten onderzoeken door gespecialiseerde functies binnen de bredere Haleon groep wereldwijd, voor zover toegestaan onder de lokale wetgeving.

### **c) Feedback**

Waar mogelijk krijgen Melders feedback over de voorgenomen of ondernomen maatregelen naar aanleiding van de Melding, waarbij altijd de van toepassing zijnde wettelijke en reglementaire verplichtingen in acht worden genomen. De Melder ontvangt doorgaans feedback binnen drie maanden nadat de Melding is gedaan.

### **2.3 Geen represailles**

In overeenstemming met de End-to-End Policy voor Bezorgdheden zal de Vennootschap geen represailles of pogingen tot represailles tolereren door een andere persoon of groep, direct of indirect, tegen iemand die, op basis van redelijke vermoedens, een Melding doet of bijstand verleent aan HR, Legal, het management van de Vennootschap of een andere persoon of groep, met inbegrip van enige overheidsinstantie, regelgevende instantie of handhavingsinstantie, die een Melding onderzoekt of anderszins bijdraagt aan het oplossen ervan.

De Vennootschap zal ook geen represailles tolereren tegen:

- derden die de Melder vertrouwelijk bijstaan bij een Melding in een werkgerelateerde context,
- personen die verbonden zijn met de Melder en die het slachtoffer kunnen worden van represailles in een werkgerelateerde context, zoals collega's of familieleden van de Melder, of
- juridische entiteiten die eigendom zijn van de Melder, waarvoor de Melder werkt, of waarmee de Melder anderszins in een werkgerelateerde context verbonden is.

(samen "**Facilitators**")

### **2.4 Extern melden**

De Vennootschap moedigt Melders aan om gebruik te maken van de interne meldingsprocedures zoals uiteengezet in de End-to-End Policy voor Bezorgdheden en de landspecifieke addenda die bij deze Policy zijn gevoegd om een Melding te doen.

Er kunnen zich ook gevallen voordoen waarin het voor Melders aangewezen is om een Melding te doen bij een externe instantie. Indien de relevante bevoegde instantie in het land van de werknemer een onafhankelijk extern meldingskanaal heeft opgezet, kunnen Melders hun bezorgdheden ook op die manier kenbaar maken. Details over de autoriteiten die bevoegd zijn om een Melding te ontvangen zijn vermeld in de landspecifieke addenda.

De Vennootschap moedigt Melders ten zeerste aan advies in te winnen voordat zij een bezorgdheid aan een extern iemand melden anders dan via de beschreven kanalen.

### **2.5 Vertrouwelijkheid**

In overeenstemming met de End-to-End Policy voor Bezorgdheden worden alle onderzoeken op vertrouwelijke wijze gevoerd, zodat informatie alleen openbaar wordt gemaakt indien zulks noodzakelijk is

om het onderzoeksmateriaal te kunnen beoordelen of anderszins wettelijk verplicht is.

De Melder krijgt gewoonlijk de gelegenheid om het afschrift of de notulen van elk telefoongesprek of elke vergadering waarin de Melder een Melding doet, te controleren en te corrigeren.

Alle documenten met betrekking tot een Melding en met betrekking tot het onderzoek en de afhandeling ervan zullen op strikt vertrouwelijke basis worden bewaard, zoals verder uiteengezet in de landspecifieke addenda hieronder en zoals vereist volgens de van tijd tot tijd geldende voorschriften van de Vennootschap inzake het bewaren van documenten.

### **3. Definities**

**Unierecht:** betekent het recht van de Europese Unie met betrekking tot (a) overheidsodrachten; (b) financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering; (c) productveiligheid en productconformiteit; (d) veiligheid van het vervoer; (e) bescherming van het milieu; (f) stralingsbescherming en nucleaire veiligheid; (g) veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn; (h) volksgezondheid; (i) consumentenbescherming; (j) bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen; (k) inbreuken waardoor de financiële belangen van de Europese Unie als bedoeld in artikel 325 van het Verdrag betreffende de werking van de Europese Unie ("**VWEU**") en nader toegelicht in relevante Uniemaatregelen worden geschaad; (l) inbreuken in verband met de interne markt, zoals bedoeld in artikel 26, lid 2, VWEU, met inbegrip van inbreuken op de Unieregels inzake mededinging en staatssteun, alsmede inbreuken in verband met de interne markt en die betrekking hebben op handelingen die in strijd zijn met de regels van de vennootschapsbelasting of constructies die erop gericht zijn een belastingvoordeel te verkrijgen dat afbreuk doet aan de strekking of het doel van het toepasselijke vennootschapsbelastingrecht.

**Represailles:** betekent represailles tegen personen die Meldingen doen en Facilitators met betrekking tot Inbreuken op het Unierecht, met inbegrip van maar niet beperkt tot: (a) schorsing, ontslag of soortgelijke maatregelen; (b) degradatie of onthouden van bevordering; (c) overdracht van taken, verandering van locatie van de arbeidsplaats, loonsverlaging, verandering van werktijden; (d) onthouden van opleiding; (e) een negatieve prestatiebeoordeling of arbeidsreferentie; (f) het opleggen of toepassen van disciplinaire maatregelen, berispingen of andere sancties, zoals een financiële sanctie; (g) dwang, intimidatie, pesterijen of uitsluiting; (h) discriminatie, nadelige of ongelijke behandeling; (i) niet-omzetting van een tijdelijke

arbeidsovereenkomst in een arbeidsovereenkomst voor onbepaalde tijd, in het geval de werknemer de gerechtvaardigde verwachting had dat hem een dienstverband voor onbepaalde tijd zou worden aangeboden; (j) niet-verlenging of vroegtijdige beëindiging van een tijdelijke arbeidsovereenkomst; (k) schade, met inbegrip van reputatieschade, met name op sociale media, of financieel nadeel, met inbegrip van omzetsderving en inkomstenderving; (l) opname op een zwarte lijst op basis van een informele of formele overeenkomst voor een hele sector of bedrijfstak, waardoor de persoon geen baan meer kan vinden in de sector of de bedrijfstak; (m) vroegtijdige beëindiging of opzegging van een contract voor de levering van goederen of diensten; (n) intrekking van een licentie of vergunning; (o) psychiatrische of medische verwijzingen.

## **LANDSPECIFIEK ADDENDUM:**

### **BELGIË**

Dit landspecifiek addendum is een aanvulling op de End-to-End Policy voor Bezorgdheden en de Europese Klokkenluiderspolicy (de "**Policy**"). In geval van tegenstrijdigheid, is dit landspecifiek addendum van toepassing.

#### **Op wie dit landspecifiek addendum lokaal van toepassing is**

Dit landspecifiek addendum is in België ingevoerd door een lokale juridische entiteit met meer dan 50 werknemers, namelijk Haleon Belgium NV, met maatschappelijke zetel te Da Vincilaan 5, 1930 Zaventem, België, BTW BE 0404.195.238, RPM/RPR Brussel ("**Haleon België**").

Dit addendum is van toepassing op werknemers van Haleon België, maar we aanvaarden ook Meldingen van personen die informatie hebben verkregen over de hieronder beschreven inbreuken in het kader van een werkgerelateerde of professionele relatie met Haleon België of een andere juridische entiteit van Haleon. De categorieën van personen die Meldingen kunnen doen uit hoofde van hun werkgerelateerde of professionele relatie omvatten, naast werknemers van Haleon België, personen met de hoedanigheid van zelfstandige, personen die werken onder toezicht en leiding van aannemers, onderaannemers, dienstverleners, leveranciers, bestuurders, functionarissen, aandeelhouders, personen die behoren tot het bestuurlijk, leidinggevend of toezichthoudend orgaan, niet-leidinggevend personeel, vrijwilligers, stagiairs, voormalige werknemers (wanneer de informatie werd verkregen tijdens hun werksrelatie) of kandidaten (wanneer zij de informatie verkregen tijdens de wervingsprocedure of andere precontractuele onderhandelingen). Daarnaast kunnen werknemers van Haleon België en derden die informatie hebben verkregen buiten de context van een werkgerelateerde of professionele relatie met Haleon België ook lokaal een interne Melding doen, op voorwaarde dat de Melding betrekking heeft op financiële diensten, producten en markten en de witwaswetgeving (gezamenlijk "**Melders**").

#### **Op welke bezorgdheden dit landspecifiek addendum lokaal van toepassing is**

In aanvulling op de onderwerpen die in deze Policy worden beschreven, behandelt dit landspecifiek addendum klachten en bezorgdheden (gezamenlijk "**Meldingen**") van werknemers, aandeelhouders en anderen die tewerkgesteld worden door of werkzaam zijn voor een van de entiteiten die in dit addendum worden genoemd en die betrekking hebben op de volgende zaken:

- inbreuken met betrekking tot elke schending van de wettelijke of reglementaire (Belgische) bepalingen of de rechtstreeks toepasbare

Europese bepalingen, evenals de bepalingen genomen in uitvoering van de voormelde bepalingen, specifiek voor: (i) overheidsopdrachten; (ii) financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering; (iii) productveiligheid en productconformiteit; (iv) veiligheid van het vervoer; (v) bescherming van het milieu; (vi) stralingsbescherming en nucleaire veiligheid; (vii) veiligheid van levensmiddelen en diervoeders, diergezondheid en dierenwelzijn; (viii) volksgezondheid; (ix) consumentenbescherming; (x) bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen; (xi) bestrijding van belastingfraude; (xii) sociale fraudebestrijding;

- inbreuken waardoor de financiële belangen van de Unie worden geschaad; en
- inbreuken in verband met de interne markt.

Informatie waarvan de bekendmaking verboden is omdat het betrekking heeft op de nationale veiligheid, omdat het gerubriceerde gegevens betreft, omdat het onder het beroepsgeheim van advocaten of het medisch beroepsgeheim valt of omdat het gedekt is door de geheimhouding van rechterlijke beraadslagingen is uitdrukkelijk uitgesloten van het toepassingsgebied van dit landspecifiek addendum, in overeenstemming met de toepasselijke wettelijke voorwaarden zoals opgesomd in artikel 5, §1 van de Wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector ("**Belgische Klokkenluiderswet**").

### **Hoe een inbreuk of bezorgdheid die onder dit lokale addendum valt intern gemeld kan worden**

In België kunnen werknemers gebruik maken van de meldingskanalen die zijn beschreven in de End-to-End Policy voor Bezorgdheden. Het gebruik van deze kanalen betekent echter dat de bezorgdheid wordt behandeld en mogelijks onderzocht met behulp van groepsmiddelen.

Indien u wenst dat uw bezorgdheid lokaal wordt behandeld en, indien van toepassing, lokaal wordt onderzocht, gelieve dan contact op te nemen met de heer Michaël Falcomer (e-mail: [Haleon.SpeakUp.Belgium@Haleon.com](mailto:Haleon.SpeakUp.Belgium@Haleon.com)) omtrent uw bezorgdheid, aangezien hij momenteel is aangesteld als lokale meldingsbeheerder ("**Lokale Meldingsbeheerder**"). In het geval dat de Lokale Meldingsbeheerder afwezig is op het werk (bijv. wegens vakantie, ziekteverlof), zal de Legal & Compliance Director hem/haar vervangen. Indien u hierom zou verzoeken wordt binnen een redelijke termijn een fysieke ontmoeting met de Lokale Meldingsbeheerder (of de door hem/haar gemachtigde persoon) georganiseerd.

In het geval dat de Lokale Meldingsbeheerder zich in een belangenconflict bevindt of het onderwerp van de Melding is, kan de Melding naar eigen keuze worden ingediend via de meldingskanalen die vermeld staan in de End-to-End Policy voor Bezorgdheden of door een e-mail te sturen naar de persoon die de Lokale Meldingsbeheerder vervangt tijdens zijn/haar afwezigheid.

Haleon kan de bijstand inschakelen van een extern advocatenkantoor om advies in te winnen over hoe verder moet worden gehandeld in overeenstemming met de lokale wetgeving.

### **Ontvangst en behandeling van interne Meldingen die lokaal zijn gedaan**

Na ontvangst van de Melding zal de Lokale Meldingsbeheerder een voorlopige beoordeling maken van de vraag of de gemelde feiten binnen het materieel toepassingsgebied van dit landspecifiek addendum vallen, evenals van de consistentie en plausibiliteit van de gerapporteerde feiten, en de Lokale Meldingsbeheerder kan u om aanvullende informatie vragen indien hij of zij dit noodzakelijk acht.

Zodra een Melding is ontvangen en de ontvangst ervan is bevestigd, zal de Lokale Meldingsbeheerder ook beoordelen of de Melding een structureel probleem aan het licht brengt of een probleem dat betrekking heeft op twee of meer entiteiten van de groep en/of alleen effectief kan worden afgehandeld met een grensoverschrijdende aanpak die Haleon België niet kan implementeren met het oog op het waarborgen van de doeltreffendheid van de Europese Klokkenluiderspolicy. Indien dit het geval is, kan de Lokale Meldingsbeheerder:

- De Melder feedback geven waarin (voor zover van toepassing) gedetailleerd wordt uiteengezet waarom het voor de Lokale Meldingsbeheerder niet mogelijk was om de Melding lokaal te onderzoeken en/of af te handelen. De Lokale Meldingsbeheerder zal de Melder vervolgens expliciet aanraden om de Melding rechtstreeks in te dienen via de meldingskanalen vermeld in de End-to-End Policy voor Bezorgdheden; of
- Toestemming vragen aan de Melder om de Melding te delen met de aangewezen groepsmiddelen. Desalniettemin blijft de Lokale Meldingsbeheerder verantwoordelijk en aansprakelijk voor alle interne Meldingen die lokaal zijn gedaan, met inbegrip voor het waarborgen van de vertrouwelijkheid, het geven van feedback en het afhandelen van de Melding. Indien de Melder geen toestemming verleent voor het delen van de Melding met de aangewezen groepsmiddelen, zal de Lokale Meldingsbeheerder de Melder feedback geven zoals beschreven in de bovenstaande paragraaf.

### **Onderzoek naar de Melding en feedback aan de Melder**

De Lokale Meldingsbeheerder leidt het onderzoek naar de Melding en bepaalt hiervoor de benodigde interne (en, voor zover de Melder hiervoor toestemming heeft gegeven, externe) middelen, evenals de personen die toegang moeten hebben tot de Melding en tot de informatie verkregen uit de Melding en uit het interne onderzoeksproces (met inbegrip van persoonsgegevens, zoals de identiteit van de Melder).

Zodra het onderzoek is afgerond, zullen de nodige maatregelen worden getroffen in overeenstemming met de policies en procedures van Haleon België en de toepasselijke lokale wetgeving.

De Lokale Meldingsbeheerder blijft verantwoordelijk voor het onderhouden van de communicatie met de Melder en kan, indien zulks nodig wordt geacht, aanvullende informatie over de Melding opvragen bij de Melder.

In elk geval zal de Lokale Meldingsbeheerder de Melder schriftelijk contacteren binnen drie (3) maanden na de initiële ontvangstbevestiging van de Melding of, indien geen ontvangstbevestiging werd ontvangen, binnen drie maanden na het verstrijken van een periode van zeven (7) kalenderdagen volgend op de Melding, om te reageren op de onderzoeksmaatregelen, waarbij samenvattende informatie wordt verstrekt over de voorgenomen of ondernomen stappen om de Melding op te volgen en aan de gemelde bezorgdheid tegemoet te komen, dit alles onder voorbehoud van de andere verplichtingen van Haleon België (bv. vertrouwelijkheid en verplichtingen inzake de bescherming van persoonsgegevens).

### **Waarborgen**

Zodra een Melding die binnen het toepassingsgebied valt is ingediend, zal de melder de waarborgen genieten die worden beschreven in hoofdstukken 6 en 7 van de Belgische Klokkenluiderswet, onder andere met betrekking tot het verbod op represailles en vertrouwelijkheid.

### **Extern melden in België**

Haleon België dringt er sterk op aan om Meldingen intern te doen zodat eventuele bezorgdheden kunnen worden opgelost. Indien u echter beslist om uw bezorgdheden extern te melden in overeenstemming met de toepasselijke wettelijke bepalingen, kunt u naast de federale coördinator ook meldingen doen bij de relevante Belgische bevoegde autoriteiten, d.w.z.:

- de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;
- de Federale Overheidsdienst Financiën;
- de Federale Overheidsdienst Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu;



- de Federale Overheidsdienst Mobiliteit en Vervoer;
- de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;
- de Programmatie Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid;
- het Federaal Agentschap voor Nucleaire Controle;
- het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;
- het Federaal Agentschap voor de veiligheid van de voedselketen;
- de Belgische Mededingingsautoriteit;
- de Gegevensbeschermingsautoriteit;
- de Autoriteit voor Financiële diensten en Markten;
- de Nationale Bank van België;
- het College van toezicht op de bedrijfsrevisoren;
- de autoriteiten gemeld in artikel 85 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;
- het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater;
- het Belgisch Instituut voor postdiensten en telecommunicatie;
- het Rijksinstituut voor ziekte- en invaliditeitsverzekering;
- het Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen;
- de Rijksdienst voor Arbeidsvoorziening;
- de Rijksdienst voor Sociale Zekerheid;
- de Sociale Inlichtingen en Opsporingsdienst;
- de Autonome dienst Coördinatie Anti-Fraude (CAF); of
- de Scheepvaartcontrole.

De manier waarop externe meldingen kunnen worden gedaan, is te vinden op de websites van de relevante bevoegde autoriteiten.

### **Verwerking van persoonsgegevens**

Alle ontvangen Meldingen zullen met gepaste vertrouwelijkheid worden behandeld en voldoen aan de huidige privacy- en gegevensbeschermingswetgeving die in elk relevant land van tijd tot tijd

van toepassing is, in het bijzonder Verordening (EU) 2016/679 (AVG) en de nationale uitvoeringswetten, in het bijzonder de Belgische Wet Bescherming Persoonsgegevens van 30 juli 2018 ("**Gegevensbeschermingswetten**").

Dit addendum verstrekt informatie met betrekking tot de verwerking van persoonsgegevens in verband met het lokale meldingskanaal voor België en vormt een aanvulling op en doet geen afbreuk aan de informatie die wordt verstrekt in Haleon's Privacyverklaring voor Werknemers [Site de communication - Belgium & Luxembourg Employee PN 18 Jul 2022.pdf - Tous les documents \(sharepoint.com\)](#) voor zover het werknemers betreft, en in de algemene [Haleon Privacy Centre](#), zoals van tijd tot tijd kan worden gewijzigd. In geval van tegenstrijdigheid tussen de informatie in dit addendum en in de relevante verklaringen inzake gegevensbescherming die hierboven worden genoemd, zal dit addendum voorrang hebben.

Gelieve de relevante informatie met betrekking tot gegevensbescherming zoals hierboven vermeld te raadplegen voor verdere informatie met betrekking tot de verwerking van persoonsgegevens door Haleon België, in het bijzonder m.b.t. ontvangers van gegevens, overdracht van persoonsgegevens buiten de EER, uw rechten en hoe en met wie u contact kunt opnemen om deze uit te oefenen.

Indien u het onderwerp bent van een Melding, wordt u geïnformeerd over de verzameling van uw persoonsgegevens in overeenstemming met de toepasselijke lokale vereisten. In overeenstemming met de toepasselijke wetgeving kan dergelijke informatie worden uitgesteld indien dit noodzakelijk is voor onderzoeks- of andere bewijsdoeleinden.

## **7. Verwerkingsverantwoordelijke**

Haleon België treedt op als verwerkingsverantwoordelijke voor de persoonsgegevens die worden verzameld en verwerkt in verband met het lokale meldingskanaal voor België.

## **8. Verwerkingsdoeleinden en wettelijke gronden**

De doeleinden voor de gegevensverwerking zijn (i) het beoordelen van de Meldingen ontvangen via het lokale meldingskanaal voor België, (ii) het voeren van de noodzakelijke interne onderzoeken, (iii) het vastleggen van de werking en doeltreffendheid van het interne en lokale meldingskanaal, (iv) het naleven van de Belgische Klokkenluiderswet en (v) het nemen van de noodzakelijke maatregelen om de ontvangen Meldingen aan te pakken.

De wettelijke gronden voor de verwerking van persoonsgegevens ontvangen naar aanleiding van een Melding of in het kader van een daaropvolgend intern onderzoek zijn artikel 6 (1) (c) van de AVG (de verwerking is noodzakelijk om te voldoen aan de wettelijke verplichting om over een intern klokkenluiderskanaal te beschikken) en artikel 6(1)(f) van

de AVG (de verwerking is noodzakelijk voor de gerechtvaardigde belangen te behartigen die Haleon België nastreeft, waaronder het onderzoeken van en het nemen van passende maatregelen in verband met een mogelijke schending van relevante wet- en regelgeving en andere zaken die binnen het toepassingsgebied vallen, waardoor zodoende naleving wordt gewaarborgd). Bij het nastreven van deze gerechtvaardigde belangen zal Haleon België deze afwegen tegen de belangen van de betrokkenen en de fundamentele rechten en vrijheden met betrekking tot de bescherming van de persoonsgegevens van de betrokkenen.

In uitzonderlijke omstandigheden, zoals wanneer Haleon België van plan is de identiteit van de Melder aan derden bekend te maken, kan Haleon België persoonsgegevens verwerken op basis van uitdrukkelijke toestemming.

Persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten worden alleen verwerkt indien dit specifiek is toegelaten door het Unierecht of de Belgische wetgeving, in het bijzonder wanneer dit noodzakelijk is om de eigen rechtszaken van Haleon België te kunnen beheren in overeenstemming met de Belgische Wet Bescherming Persoonsgegevens.

Indien een Melding bijzondere categorieën van persoonsgegevens bevat, worden dergelijke gegevens alleen verwerkt (i) indien de verwerking noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van Haleon België of de betrokkene op het gebied van arbeidsrecht en socialezekerheids- en socialebeschermingsrecht, voor zover zulks is toegestaan bij Unierecht of Belgisch recht of door een collectieve overeenkomst op grond van Belgisch recht die passende waarborgen biedt voor de grondrechten en de fundamentele belangen van de betrokkene (Artikel 9 (2) (b) GDPR), of (ii) indien de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van rechtsvorderingen (Artikel 9 (2) (f) GDPR).

Indien bijzondere categorieën van persoonsgegevens of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten in een Melding worden opgenomen, maar duidelijk niet relevant zijn voor de gerapporteerde zaak, zullen deze onmiddellijk en veilig worden verwijderd.

Er vindt geen geautomatiseerde besluitvorming, waaronder profilering, plaats in het kader van het gebruik van het lokale meldingskanaal voor België.

## **9. Categorieën van verwerkte persoonsgegevens**

De volgende categorieën van persoonsgegevens kunnen worden verzameld en verwerkt door het gebruik van het lokale meldingskanaal voor België:

- de identiteit, functies en contactgegevens van de Melder, het/de onderwerp(en) van de Melding en de personen die betrokken zijn bij

(en geïdentificeerd zijn in verband met) de verwerking van de gemelde feiten en het verdere onderzoek daarnaar;

- gemelde inbreuken en daarmee samenhangende feiten (met inbegrip van gegevens met betrekking tot fraude of beschuldigingen van fraude, of andere overtredingen van het recht, of met betrekking tot vermoedelijke of mogelijke strafbare feiten), mededelingen en informatie verzameld/geanalyseerd in verband met het meldproces en het onderzoek van de gemelde feiten (met inachtneming van de toepasselijke vereisten onder de toepasselijke wetgeving), en het onderzoeksverslag;
- gevolgen van het onderzoek, met inbegrip van mogelijke disciplinaire maatregelen en strafrechtelijke beschuldigingen, vervolgingen of veroordelingen, indien van toepassing;
- bescherming van de relevante personen tegen represailles;
- opvolging van de Melding.

Het niet gebruiken van het lokale meldingskanaal voor België heeft geen gevolgen en het verstrekken van persoonsgegevens is vrijwillig. Het niet verstrekken van persoonsgegevens kan echter wel tot vertraging leiden of het onmogelijk maken voor Haleon België om actie te ondernemen naar aanleiding van een ingediende Melding, maar heeft geen andere gevolgen.

De bron waarvan de persoonsgegevens afkomstig zijn, is meestal de persoon op wie ze betrekking hebben (bv. de werknemers zelf) en persoonsgegevens die Haleon België op een geoorloofde manier ontvangt van publiek beschikbare bronnen en/of van derden zoals hieronder verder wordt beschreven.

Haleon België kan persoonsgegevens verzamelen op de hierna vermelde manieren:

- Het verzamelen van persoonsgegevens rechtstreeks van de betrokkene, zoals door middel van een Melding of andere vormen van informatie die betrokkenen aan Haleon België verstrekken in verband met hun tewerkstelling;
- Het verzamelen van persoonsgegevens tijdens de activiteiten van de betrokkenen in het kader van hun tewerkstelling, zoals door hun prestaties en interactie met andere werknemers, klanten of andere personen; en
- Het verzamelen van persoonsgegevens van andere partijen zoals Melders en andere werknemers.

## **10. Vertrouwelijkheid**

Uw identiteit wordt op een vertrouwelijke wijze verwerkt. Dit betekent dat uw identiteit aan niemand anders wordt bekendgemaakt dan aan de gemachtigde medewerkers die bevoegd zijn om Meldingen te ontvangen of op te volgen, behalve indien het gaat om een noodzakelijke en evenredige verplichting krachtens het Unierecht of de nationale wetgeving in het kader van onderzoek door nationale autoriteiten of gerechtelijke procedures, of met uw uitdrukkelijke toestemming. Dit geldt ook voor alle andere informatie waaruit uw identiteit direct of indirect kan worden afgeleid. In geval van openbaarmaking op grond van een verplichting uit hoofde van het Unierecht of nationaal recht in het kader van een onderzoek door nationale autoriteiten of een gerechtelijke procedure, wordt u daarvan vooraf in kennis gesteld, tenzij die informatie de gerelateerde onderzoeken of gerechtelijke procedures in gevaar zou brengen.

## **11. Bewaringstermijnen**

Persoonsgegevens die duidelijk niet relevant zijn voor de behandeling van een specifieke melding, worden niet verzameld, of worden, indien onbedoeld verzameld, onmiddellijk gewist. Meer in het algemeen worden persoonsgegevens niet langer bewaard dan noodzakelijk en proportioneel is voor het doel waarvoor ze zijn verzameld, in overeenstemming met de toepasselijke wetgeving en de voorschriften van de Vennootschap voor het bewaren van documenten zoals van tijd tot tijd van toepassing.

Meldingen, met inbegrip van opnames, afschriften en notulen, zullen enkel bewaard worden zolang als strikt noodzakelijk en proportioneel is voor het onderzoek en voor de bescherming van de Melder, de personen die het onderwerp zijn van de Melding en alle derden die in de Melding vermeld worden, rekening houdend met de tijd die nodig is voor verder onderzoek en de specifieke bewaringstermijnen voorzien in de Belgische Klokkenluiderswet zoals hieronder beschreven. In het bijzonder zullen persoonsgegevens met betrekking tot Meldingen die buiten het toepassingsgebied vallen zonder onmiddellijk worden gewist.

In overeenstemming met Artikel 22, §1 van de Belgische Klokkenluiderswet, zullen Meldingen bewaard worden voor de duur van de werkgerelateerde relatie van de Melder met Haleon België. De naam, functie en contactgegevens van de Melder en van elke persoon tot wie de beschermings- en ondersteuningsmaatregelen onder de Belgische Klokkenluiderswet zich uitstrekken, evenals de personen die het onderwerp zijn van de Melding en elke derde die in de Melding worden vermeld, met inbegrip van, indien van toepassing, hun ondernemingsnummer, zullen worden bijgehouden tot wanneer de gemelde inbreuk is verjaard, zoals vereist onder Artikel 21 van de Belgische Klokkenluiderswet.

Als er naar aanleiding van een Melding een disciplinaire of gerechtelijke procedure wordt gestart, worden de persoonsgegevens met betrekking tot

de Melding in ieder geval bewaard tot het einde van de procedure of het einde van de vervaltermijn voor beroep tegen de beslissing.

Bovendien kan Haleon België persoonsgegevens met betrekking tot een Melding tot vijf (5) jaar bewaren, in tussentijdse opslag, indien daartoe een wettelijk verplichting zou bestaan (bijvoorbeeld om te voldoen aan boekhoudkundige, sociale of fiscale verplichtingen).

## **12. Rechten in het kader van gegevensbescherming**

Betrokkenen kunnen hun recht op toegang, rectificatie, wissing, overdracht (overdraagbaarheid), beperking van de verwerking en bezwaar uitoefenen zoals beschreven in de hierboven vermelde relevante verklaringen over gegevensbescherming. Ze hebben ook het recht om hun toestemming op elk moment in te trekken en klachten in te dienen bij de bevoegde gegevensbeschermingsautoriteit. In België is dit de Belgische Gegevensbeschermingsautoriteit (<https://www.dataprotectionauthority.be>).

## 6.2 Polska

Niniejsza sekcja dotycząca Polski („**Sekcja**”) została opracowana zgodnie z ustawą z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. Nr 2024 poz. 928) („**Ustawa o ochronie sygnalistów**”). Stanowi ona uzupełnienie Polityki dotyczącej kompleksowego rozpatrywania zgłoszonych zastrzeżeń (*End-to-End Concerns Policy*) oraz Polityki w zakresie sygnalizowania naruszeń w UE (*EU Whistleblowing Policy*) (łącznie „**Polityka**”). W przypadku jakichkolwiek rozbieżności, niniejsza Sekcja ma charakter rozstrzygający.

### **Osoby, do których niniejsza Sekcja ma zastosowanie na poziomie lokalnym**

Niniejsza Sekcja obowiązuje w Polsce w podmiotach prawnych Haleon zatrudniających co najmniej 50 osób (łącznie „**Haleon Poland**”).

Niniejsza Sekcja ma zastosowanie do obecnych lub byłych pracowników Haleon Poland (zatrudnionych na stałe, tymczasowo, w pełnym wymiarze czasu pracy, w niepełnym wymiarze czasu pracy lub na czas określony) oraz innych osób, które uzyskały informacje o Naruszeniach (zdefiniowanych poniżej) w kontekście związanym z pracą (stosunki pracownicze lub zawodowe lub świadczenie usług na rzecz Haleon Poland). Do tego grona należą osoby prowadzące obecnie lub przeszłości działalność gospodarczą, aktualni lub byli podwykonawcy, usługodawcy, dostawcy, członkowie organów kierowniczych, kontrolnych lub nadzorczych oraz prokurenci, wspólnicy i akcjonariusze, pracownicy agencji, osoby odbywające praktyki zawodowe, wolontariusze, stażyści, praktykanci oraz osoby pracujące pod nadzorem wykonawców, dostawców, usługodawców i ich podwykonawców, w tym na podstawie umowy cywilnoprawnej. Niniejsza Sekcja ma również zastosowanie do osób, które zgłaszają naruszenie, o którym dowiedziały się podczas procesu rekrutacji lub w trakcie negocjacji poprzedzających zawarcie umowy (łącznie „**Zgłaszający**”).

### **Do jakich zastrzeżeń odnosi się niniejsza Sekcja na poziomie lokalnym**

Niniejsza Sekcja dotyczy zgłaszania skarg i zastrzeżeń (łącznie „**Zgłoszenia**”) dotyczących działania lub zaniechania niezgodnego z prawem lub mającego na celu obejścia prawa, dotyczących (a) korupcji; (b) zamówień publicznych; (c) usług, produktów i rynków finansowych; (d) przeciwdziałaniu zapobieganiu praniu pieniędzy i finansowaniu terroryzmu; (e) bezpieczeństwa produktów i ich zgodności z wymogami; (f) bezpieczeństwa transportu; (g) ochrony środowiska; (h) ochrony radiologicznej i bezpieczeństwa jądowego; (i) bezpieczeństwa żywności i pasz; (j) zdrowia i dobrostanu zwierząt; (k) zdrowia publicznego; (l)

ochrony konsumentów; (m) ochrony prywatności i danych osobowych; (n) bezpieczeństwa sieci i systemów teleinformatycznych; (o) interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, dowolnej jednostki samorządu terytorialnego lub Unii Europejskiej; (p) rynku wewnętrznego Unii Europejskiej, w tym publicznoprawnych zasad konkurencji i pomocy publicznej oraz opodatkowania osób prawnych; (r) konstytucyjnych wolności i praw człowieka i obywatela występujących w kontaktach jednostki z organami władzy publicznej (łącznie „**Naruszenia**”).

Niniejsza Sekcja dotyczy wyłącznie Zgłoszeń, w odniesieniu do których (a) Zgłaszający ujawnił Haleon Poland swoją tożsamość, oraz (b) Zgłaszający miał uzasadnione podstawy sądzić, że informacje zawarte w Zgłoszeniu: (i) są prawdziwe w momencie dokonywania Zgłoszenia, oraz (ii) mieszczą się w zakresie Naruszeń wskazanych powyżej.

Niniejsza Sekcja nie obejmuje zgłoszeń anonimowych i zgłoszeń dotyczących indywidualnych spraw pracowniczych, a także skarg dotyczących wyników pracy lub skarg związanych z warunkami zatrudnienia (chyba że wchodzi one w zakres Naruszeń wskazanych powyżej). Tego rodzaju kwestie co do zasady nie wchodzi w zakres niniejszej Sekcji i lepszym rozwiązaniem może być zgłoszenie ich na podstawie innej polityki lub procedury obowiązującej w Haleon Poland.

### **Jak wewnętrznie zgłosić Naruszenie lub zastrzeżenia objęte zakresem niniejszej Sekcji na poziomie lokalnym**

W Polsce, w celu zgłaszania zastrzeżeń na podstawie Polityki dotyczącej kompleksowego rozpatrywania zgłoszonych zastrzeżeń (*End-to-End Concerns Policy*), Zgłaszający mogą korzystać z kanałów zgłaszania określonych w Polityce dotyczącej kompleksowego rozpatrywania zgłoszonych zastrzeżeń (*End-to-End Concerns Policy*). Jednak korzystanie z tych kanałów oznacza, że zgłoszenie zostanie odebrane i potencjalnie zbadane przy użyciu zasobów grupy zgodnie z Polityką dotyczącą kompleksowego rozpatrywania zgłoszonych zastrzeżeń (*End-to-End Concerns Policy*), a zatem postanowienia niniejszej Sekcji i przepisy Ustawy o ochronie sygnalistów nie będą miały zastosowania.

Osoby, które chcą, aby ich zgłoszenia Naruszeń zostały odebrane i w stosownych przypadkach zbadane lokalnie zgodnie z niniejszą Sekcją i zgodnie z Ustawą o ochronie sygnalistów, proszone są o skorzystanie z jednego z lokalnych kanałów zgłoszeń wskazanych w niniejszej Sekcji, tj:

- a) wysłanie wiadomości e-mail do lokalnego Działu Postępowań Wyjaśniających na adres: [[Whistleblower.Poland@Haleon.com](mailto:Whistleblower.Poland@Haleon.com)], lub
- b) osoby, które chciałyby dokonać Zgłoszenia osobiście, proszone są o kontakt z dowolnym członkiem lokalnego Działu Postępowań Wyjaśniających pod adresem:



[[Whistleblower.Poland@Haleon.com](mailto:Whistleblower.Poland@Haleon.com)] lub na jej/jego służbowy adres e-mail (w trybie prywatnym). Spotkanie zostanie zorganizowane jak najszybciej, nie później niż w terminie 14 dni od otrzymania takiej prośby.

Otrzymanie Zgłoszenia zgodnie z niniejszą Sekcją zostanie potwierdzone w terminie 7 (siedmiu) dni od dnia jego otrzymania, chyba że Zgłaszający nie poda adresu do doręczeń lub adresu e-mail, na który takie potwierdzenie można przekazać.

Zgłoszenia dokonane za pośrednictwem lokalnych kanałów zgłoszeń na podstawie niniejszej Sekcji będą przyjmowane, zarządzane i (jeśli spełnione zostaną warunki wstępne) rozpatrywane przez lokalny Dział Postępowań Wyjaśniających, który jest upoważniony przez Haleon Poland do przyjmowania i podejmowania działań następczych dotyczących Zgłoszeń dokonanych na podstawie niniejszej Sekcji.

Lokalny Dział Postępowań Wyjaśniających składa się z 1 (jednego) do 3 (trzech) członków, którzy są powoływani przez Zarząd Haleon Poland. Obecnie jedynym członkiem lokalnego Działu Postępowań Wyjaśniających jest: Pan Marcin Jaworski (Marcin.Jaworski@Haleon.com). Skład lokalnego Działu Postępowań Wyjaśniających może ulegać zmianie. Aktualny skład lokalnego Działu Postępowań Wyjaśniających jest dostępny na portalu intranetowym Haleon Poland.

W celu zapewnienia rzetelnego i prawidłowego postępowania, Haleon Poland może zwrócić się o pomoc do dalszych ekspertów lub doradców zewnętrznych.

### **Procedura wyjaśniająca i informacje zwrotne**

Po otrzymaniu Zgłoszenia zgodnie z niniejszą Sekcją, lokalny Dział Postępowań Wyjaśniających przeprowadzi wstępną ocenę Zgłoszenia w celu ustalenia, czy istnieją dowody *prima facie* na wystąpienie Naruszenia, a jeśli tak, to zostaną podjęte odpowiednie czynności, które mogą obejmować postępowanie wyjaśniające. Wszystkie działania następcze będą podejmowane z zachowaniem należytej staranności. Zgłaszający może zostać poproszony o przekazanie dodatkowych informacji w związku z takim postępowaniem wyjaśniającym.

Haleon Poland będzie dążyć do informowania Zgłaszającego o przebiegu każdego postępowania wyjaśniającego i jego prawdopodobnych ramach czasowych. Czasami jednak potrzeba zachowania poufności może uniemożliwić nam przekazanie Zgłaszającemu szczegółowych dodatkowych informacji na temat postępowania wyjaśniającego lub działań podjętych w jego wyniku. Haleon Poland będzie za każdym razem przekazywać informację zwrotną na temat planowanych lub podjętych działań następczych w związku ze Zgłoszeniem oraz powodów takich działań, w terminie 3 (trzech) miesięcy od potwierdzenia przyjęcia Zgłoszenia lub od

terminu na potwierdzenie jego przyjęcia (w przypadku nieprzekazania potwierdzenia). Zgłaszający jest zobowiązany do traktowania wszelkich informacji dotyczących postępowania wyjaśniającego jako ściśle poufnych.

### **Anonimowość i poufność**

Haleon Poland podejmie działania mające na celu zachowanie poufności wszystkich zaangażowanych stron, w zakresie, w jakim jest to wymagane przez prawo w danych okolicznościach. Haleon Poland nie ujawni żadnej nieupoważnionej osobie, bez wyraźnej zgody Zgłaszającego, jego tożsamości ani żadnych informacji, z których można bezpośrednio lub pośrednio wywnioskować jego tożsamość.

Zakaz ujawniania nie będzie miał zastosowania, jeżeli:

- a) ujawnienie jest koniecznym i proporcjonalnym obowiązkiem wynikającym z przepisów prawa w związku z postępowaniami wyjaśniającymi prowadzonymi przez organy publiczne lub postępowaniami sądowymi, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy Zgłoszenie; lub
- b) ujawnienie jest wymagane zgodnie z prawem na innej podstawie.

Bezpośrednie lub pośrednie działania odwetowe wobec osób dokonujących Zgłoszeń oraz osób, które ułatwiają dokonanie Zgłoszenia lub w inny sposób pomagają w dokonaniu Zgłoszenia lub w przeprowadzeniu postępowania wyjaśniającego, nie będą tolerowane. Haleon Poland uznaje wszystkie formy działań odwetowych określone w Ustawie o ochronie sygnalistów.

### **Złośliwe lub fałszywe Zgłoszenia**

W przypadku stwierdzenia, że dana osoba świadomie zgłosiła nieprawdziwe informacje, wobec takiej osoby mogą zostać podjęte działania dyscyplinarne.

### **Zgłoszenia zewnętrzne na poziomie lokalnym**

Haleon Poland zachęca do dokonywania Zgłoszeń wewnętrznie, aby umożliwić wyjaśnienie wszelkich zastrzeżeń. Zgłaszający może jednak dokonać Zgłoszenia zewnętrznie poprzez zewnętrzne kanały zgłoszeń, do których należą: naczelne i centralne organy administracji państwowej, organy administracji samorządowej oraz inne organy państwowe, prezydent miasta, starosta, marszałek województwa, regionalne izby obrachunkowe, a także instytucje, organy lub agencje Unii Europejskiej, stosownie do ich właściwości. W przypadku, gdy Zgłaszający nie jest w stanie zidentyfikować właściwego organu, Zgłoszenia mogą być kierowane do Rzecznika Praw Obywatelskich.

## **Dokumentacja**

Haleon Poland będzie przechowywać dokumentację wszystkich Zgłoszeń dokonanych zgodnie z niniejszą Sekcją. Dokumentacja będzie przechowywana przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze lub po zakończeniu postępowań zainicjowanych tymi działaniami.