TOWERS WATSON LIFESIGHT OFP
Pension Funding Organisation
Institution for occupational retirement provision authorised as of 25 August 2015 (FSMA 50.616)
Da Vincilaan 5 | Building Caprese | 1930 Zaventem | Belgium
Compnay number 629 749 932

Procedure for reporting Breaches (Whistleblower policy)

1. Introduction

The Law of 28 November 2022[1] (hereby the "whistleblower law") requires each occupational retirement institution (IORP) to have an effective procedure for reporting Breaches that provides enhanced protection for individuals who report Breaches, in good faith, in or outside a professional context, without going through the normal reporting channels.

Any "whistleblower" referred to in article 2 must have the possibility to report to a competent person within the IORP, including reasonable suspicions, in confidence and without fear of reprisal, about actual or potential Breaches so that the IORP can take appropriate action in case of potential or actual Breaches of legal and regulatory provisions as listed in article 3 of this document, which have occurred or are very likely to occur, as well as regarding attempts to conceal such Breaches.

This document describes the procedure, which is approved by the IORP, and which is intended to give every person referred to in article 2 the opportunity to report (potential) Breaches to the IORP so that the IORP can take appropriate action.

2. Concerned persons - Whistleblowers

This internal reporting procedure refers to:

- those involved in a work-related context with the IORP, in particular those involved in the management of the IORP[2] (actual, former and people whose working relationship has yet to start):
    - the (former) members of the General Assembly and their (former) representatives;
    - the (former) members of the Board of Directors;
    - the members of the Daily Management Committee (including the Pension Fund Coordinator);
    - the (former) members of the Investment Committee;
    - the members of any other operational bodies that may be set up in future;
    - the (former) key function holders;
    - the (former) employees of the external service providers and the (former) members of the sponsors (including volunteers, (un)paid trainees, persons having a self-employed status) who are involved in the management of the IORP or rendering services to the IORP;

[1] See the law of 28 November 2022 on the protection of persons who report violations of European Union or national law within a legal entity in the private sector.
[2] Whether it is current or past, or whether it has not yet begun (in the latter case, when information about violations has been obtained during the recruitment process or other pre-contractual negotiations).

- any persons working under the supervision and direction of (sub)contractors and suppliers of the IORP;

- the whistleblowers who transmit information obtained outside of a work-related context when reporting a Breach in the field of financial services, products and markets and Breaches in the field of the prevention of money laundering and terrorist financing.

3. Concerned Breaches

"Breaches" means acts or omissions that are unlawful and relate to the areas listed below or acts that, while not necessarily unlawful, defeat the object or the purpose of the rules provided for in one or more areas listed below:

Belgian law	1. Public procurement 2. Financial services, products and markets, and prevention of money laundering and terrorist financing 3. Protection of privacy and personal data, and security of network and information systems 4. Product safety and compliance 5. Fight against tax evasion 6. Fight against welfare fraud	7. Radiation protection and nuclear safety 8. Public health 9. Transport safety 10. Consumer protection 11. Food and feed safety, animal health and welfare 12. Protection of the environment
European law	Breaches affecting the financial interests of the European Union as referred to in article 325 of the Treaty on the Functioning European Union (TFEU), i.e. mainly the fight against fraud to the European Union's financial interests, or when it concerns the internal market as referred to in article 26 §2 of the TFEU, i.e. the free movement of goods, persons, services and capital, including in competition and state aid matters	

"Financial services, products and markets" refers, among others, to the laws and regulations provisions referred to in article 45 of the law of 2 August 2002 on the supervision of the financial sector and financial services, and for which the FSMA monitors the compliance. In particular:

- The WAP (the law of 28 April 2003 on supplementary pensions and the tax regime applicable to such pensions and to certain additional social security benefits);
- The WIBP (the law of 27 October 2006 relating to the Supervision of Institutions for Occupational Retirement Provision);
- The law of 10 May 2007 related to the fight against discrimination between women and men;
- The law of 30 July 1981 related to the fight against certain acts inspired by racism or xenophobia;
- The law of 5 March 2002 on the principle of non-discrimination in favor of part-time workers;
- The law of 5 June 2002 on the principle of non-discrimination in favor of workers with a fixed-term employment contract;

- The law of 2 August 2002 on the supervision of the financial sector and financial services;
- The Law of 18 September 2017 on the prevention of money laundering and terrorist financing and limiting the use of cash;
- The law of 2 June 2021 on various financial provisions relating to the fight against fraud;
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;

This list is subject to change as new laws are passed and existing laws are amended.

Where a Law is referred to, its implementing order(s) are also referred to without needing to be specified.

When the reporting concerns an area that is not mentioned above, there is no valid internal reporting and no protection.

4. Reporting process

There are several procedures for reporting suspected or actual Breaches. The IORP encourages reporting through internal reporting channels before going through external reporting channels.

The whistleblower must behave in good faith. This means that (s)he should have reasonable grounds to believe that the information reported on Breaches were true at the time of the reporting and that it fell within the scope of the legislation in force (as described above).

If it turns out that the whistleblower has knowingly reported or publicly disclosed false information, (s)he is liable to (criminal) penalties provided in the law and will be required to compensate the victims for the resulting damage. The whistleblower also loses the benefit of the safeguards mentioned under point 7 of this procedure.

a. Internal reporting process

The persons referred in article 2 are requested to report any actual or potential Breach listed in article 3 of which they are aware by contacting the whistleblowing officer.

The whistleblowing officer is the compliance officer of the IORP, as identified in Annex 2

If the reporting relates to a Breach that involves the whistleblowing officer herself or if the whistleblower is the whistleblowing officer herself, the latter is replaced by the Chairman of the Board of Directors of the IORP, who then acts as the "back up" whistleblowing officer. This is identified in Annex 2.

Reporting can be done in writing and/or orally, anonymously or in complete confidence.

The whistleblowing officer will ask the whistleblower to provide the following information or documents (if available): the facts related to the Breach (actual or potential), the name and, if applicable, the function

of the person or institution accused of committing the Breach, the time of the Breach, any evidence of the Breach, and any other information that appears relevant to the whistleblowing officer.[3]

It is possible to report in writing by regular mail and/or email.

Reporting can also be done orally via telephone or other voice mail systems and, if requested by the whistleblower, through a face-to-face meeting within a reasonable time frame.

When a report is orally transmitted, the rules in article 5.c. apply.

Anonymous internal reports are allowed.

The whistleblowers are encouraged to provide their identity to the whistleblowing officer, based on the understanding that it will be kept confidential and will only be known by the whistleblowing officer and will not be disclosed unless the whistleblower freely and expressly gives consent or required by law. Providing the identity will allow the whistleblowing officer to inform the whistleblower of his (her) rights and duties and to ask him (her) for additional information if necessary.

b. External reporting process

Whistleblowers can use the external reporting channel to report any Breach to a competent authority responsible for receiving reports in accordance with the law and for providing them with feedback, depending on the area concerned, either after reporting through the internal channels or by directly using the external reporting channels if they consider it more appropriate.

The list of Belgian competent authorities and the references to the procedures and measures of protection for external reporting is available on the federal coordinator's website: https://www.mediateurfederal.be/en.

If reporting is done directly through the external channels, the IORP encourages to also report (potential) Breach to the whistleblowing officer (anonymously in accordance with this document), so that the IORP can also take all necessary measures internally to deal with this (potential) Breach and prevent or limit any possible (further) damage.

In accordance with the law, the FSMA has set up an easily identifiable and accessible page with clear and easily accessible information on external reporting: https://www.fsma.be/fr/faq/point-de-contact-lanceurs-dalerte

The law has also set up an external reporting channel which FSMA monitors: https://www.fsma.be/en/whistleblowing

5. Treatment of the reporting

[3] The whistleblower is asked not to provide information or personal data that is clearly not relevant to the processing of a specific report. For example, it is not necessary to provide information on the health status of a person who is the subject of a report if this health status has nothing to do with the Violation in question.

Each report will be treated with the utmost confidentiality and without retaliation. Retaliation is strictly prohibited and is closely monitored by the IORP's whistleblowing officer. The whistleblowing officer must be independent and cannot have a conflict of interest.

a. Investigation

The whistleblowing officer shall send an acknowledgement of receipt to the whistleblower within seven days of receiving the report.

If the report is made anonymously, the whistleblowing officer will not be able to acknowledge or provide feedback to the whistleblower.

The whistleblowing officer records the report in a dedicated reporting register and informs the chairman of the Board of Directors. Reports are kept for the duration of the corresponding work relationship with the whistleblower. After the legal retention period, all data will be deleted.

The whistleblowing officer performs a preliminary investigation, in accordance with the principles of confidentiality, impartiality and fairness towards all persons involved. The whistleblowing officer may contact the whistleblower to obtain further information and/or evidence regarding the Breach. (S)he may also contact any person who may have information or documents that are relevant to the investigation. (S)he shall seek the opinions of the responsible for key functions and/or the DPO, depending on their area of control, and if they are not in a conflict of interests situation. In this case, the whistleblowing officer will share information with the person(s) contacted, protecting as much as possible the identity of the whistleblower and the person reported, as well as the alleged facts. S(h)e may be assisted by third parties when (s)he deems it necessary and if they are not in a conflict of interests situation.

The results of this investigation are summarized in a written report which is provided to the chairman of the Board of Directors and is registered in the reporting register.

b. Follow-up

If the investigation reveals serious evidence of Breach, the chairman of the Board of Directors refers the matter to the Board of Directors which will decide what action should be taken.

The whistleblowing officer is informed of the decision made by the Board of Directors.

Whether the report gave rise to a follow up or whether no actions were taken, the consequences and the reasons should be recorded in the reporting register.

The whistleblowing officer shall provide feedback (on the measures envisaged or taken as follow-up and on the reasons for such follow-up) within a period not exceeding three months from the acknowledgement of receipt of the reporting (or, in the absence of an acknowledgement sent to the whistleblower, three months from the expiration of the seven-day period following the reporting).

If the Board of Directors' eventual decision following the whistleblowing officer’s report is later than this three-month period, the whistleblowing officer will provide further feedback to the whistleblower.

The whistleblowing officer will always consider whether the FSMA or any other official body should be informed of the Breach.

c. Archiving

Where an oral report by a recorded phone line or other recorded voice message system is used, with the consent of the whistleblower, the IORP shall have the right to record in one of the following ways:

- by making a recording of the conversation in a durable and retrievable form; or
- by a full and accurate transcript of the conversation made by the whistleblowing officer.

In the case of an oral report by telephone line or other non-recorded messaging system, the whistleblowing officer shall have the right to record the oral report only in the form of an accurate record of the conversation made by the whistleblowing officer.

When a person requests a meeting with the IORP whistleblowing officer, in order to make an internal report, the IORP shall ensure, with the consent of the whistleblower, that the meeting is fully and accurately recorded in one of the following forms

- by making a recording of the conversation in a durable and retrievable form; or
- by an accurate record of the meeting made by the whistleblowing officer.

The whistleblowing officer shall give the caller the opportunity to check, correct and approve the transcript of the call or the record of the conversation by signing it.

6. Protection of privacy

The reporting is processed in compliance with the privacy and data protection legislation and with Annex 1 on the processing of personal data within the framework of an internal reporting.

The IORP is the controller of the personal data processed within the framework of the internal reporting procedure. The name, position and contact details both of the reporter and any person to whom the protection and support measures extend and of the data subject, including, where applicable, the company number, shall be kept until the time when the reported breach is time-barred.

Personal data that is clearly not relevant to the handling of a specific report shall not be collected or, if collected unintentionally, shall be deleted immediately.

The reporting register is only accessible to the whistleblowing officer and the FSMA. The identity of the informant is anonymized.

7. Protective measures towards the whistleblower

IORP wants to create a safe environment where a whistleblower feels comfortable reporting any Breach within IORP. Therefore, the following safeguards have been put in place:

Confidentiality of the whistleblower's identity	**The prohibition of any form of retaliation against the whistleblower and related parties**
• Referrals are managed by the whistleblowing officer and records are kept in a location that is accessible only to authorized individuals on the investigation team; • All internal and external parties involved in the investigation and follow-up actions are subject to confidentiality obligations. Unauthorized disclosure of investigative, reporting, or reporting party information will not be tolerated and may result in sanctions, including civil or criminal prosecution. • The whistleblower's identity will **not** be disclosed, unless: (i) The whistleblower explicitly consents to disclosure; or (ii) Disclosure is required by law However, a whistleblower shall be informed before his or her identity is disclosed, unless such information would jeopardize the investigations or legal proceedings concerned.	No form of "retaliation", including a threat or attempt (such as termination or non-renewal of contract or term of office, dismissal, or equivalent actions, etc.) will be exercised by the IORP against: • the whistleblower; • a facilitator, (which is an individual who assists a whistleblower in the reporting process and whose process and whose assistance should be confidential); • third parties who are connected to whistleblowers and who are at risk of retaliation in a professional context, such as colleagues or relatives of the whistleblowers, and as well legal entities owned or operated by the whistleblowers or with whom they are associated or with whom they have a professional relationship, such as a management company. If a whistleblower or any such person fears retaliation or feels that he or she has already been retaliated against, he or she is encouraged to report his or her concerns promptly to the whistleblowing officer.

If a whistleblower or any such person fears retaliation or feels that retaliation has already been taken against him or her, he or she is encouraged to report his or her concerns to the whistleblowing officer without delay.

The whistleblower (or the persons assisting them) who believes he or she has been victimised or threatened with retaliation may lodge a reasoned complaint with the Federal Ombudsman, using the information provided under section 4.b of this procedure.

Any person who becomes a victim of retaliation has the right to file an appeal before the Labour Court in accordance with Article 578 of the Judicial Code.

8. Communication of the present procedure

The IORP is in charge of communicating the present procedure to suppliers and responsible for key functions, to the members of the operational bodies and the General Assembly and to the sponsoring companies. The IORP also ensures that this procedure is made public via the channels that it deems most appropriate.

IORP's suppliers must commit to communicate the present procedure to each member of their staff working for the IORP.

The Board of Directors will review this policy on a regular basis, at least every three years, or sooner if significant events occur. If necessary, the Board of Directors will update the policy.

This internal procedure was approved by the Board of Directors on 17 March 2023

Els De Jaeger	Sven Schroven
Chairman of the Board of Directors	Vice- President of the Board of Directors
Towers Watson LifeSight OFP	Towers Watson LifeSight OFP

Annex 1: processing of personal data within the framework of an internal reporting

This annex explains how the IORP handles the personal data of the whistleblower, of a person who is the subject of a report or any other third party mentioned on that occasion. It should be read in conjunction with the IORP's generic privacy notice which is available on https://www.lifesight.com/privacy-policy, or on request in both cases.

Concerning the whistleblower (article 13 GDPR)		
Purposes	The data transmitted to the IORP is used to send an acknowledgement of receipt of the report to the whistleblower, normally within the 7 days of receiving the report. The data is also processed for the purpose of the follow-up of the report, i.e. any action taken by the whistleblowing officer and the investigation team, or any competent authority, in order to assess the accuracy of the allegations made in the report, and, if necessary, to remedy the reported Breach.	
Legal bases	The IORP is legally required by the law of 28 November 2022 on the protection of persons who report violations of European Union or national law within a legal entity in the private sector to install a procedure for reporting breaches. The whistleblower has consented to the processing of such data (article 6.1.a) GDPR).	
Categories of data	This may include name, position, relationship to the IORP, information about the Breach (whether or not it is a criminal offense), and information about sanctions.	
Period	When the report results in a confirmed Breach	Until the reported Breach is expired, including the prescription of pleas against a judicial, administrative or other decision. In case of criminal proceedings: 5 years for offences. In case of civil liability: 5 years. In case of contractual liability: 10 years. Data needed to fulfill the internal recording obligation is kept for the duration of the corresponding work relationship with the whistleblower.
	When no actual Breach is established as a result of the report	Destruction or anonymization of data within 2 months from the end of the investigation (i.e. from the moment the Board of Directors has decided to do so), with the exception of data that allow the fulfillment of the requirement to keep reports for the duration of the corresponding work relationship with the whistleblower.
Recipients	The communication of the data of the whistleblower is necessary to the IORP and, if required, to competent authorities. This data may also be communicated, in whole or in part, to the person who is the subject of the report or to other third parties mentioned in the report in the cases provided for by the legislation in force.	

Concerning the person who is the subject of the report or any other third party mentioned on that occasion (article 14 GDPR)		
Purposes	The data transmitted to the IORP regarding the person who is the subject of the report of any other third party mentioned on that occasion is used in order to verify whether a Breach has been committed by the person who is the subject of the report.	
Categories of data	At the stage of issuing the report	The data collected and processed are those that allow the identification of the person who is the subject of the report or any other third party mentioned on this occasion. This may include their name, position, relationship to the IORP, information about the Breach (whether or not it is a criminal offence), and information about sanctions.
	At the stage of investigation of the report	In the event that an investigation is launched for the purpose of verifying the facts alleged by the whistleblower, all necessary data regarding the investigation and the adoption of appropriate measures to remedy the Breach may be collected, including reports of the verification operations, the follow-up of the report and the reporting mail.
Period	When the report results in a confirmed Breach	Until the reported Breach is expired, including the prescription of pleas against a judicial, administrative or other decision. In case of criminal proceedings: 5 years for offences. In case of civil liability: 5 years. In case of contractual liability: 10 years. Data needed to fulfill the internal recording obligation is kept for the duration of the corresponding work relationship with the whistleblower.
	When no actual Breach is established as a result of the report	Destruction or anonymization of data within 2 months from the end of the investigation (i.e. from the moment the Board of Directors has decided to do so), with the exception of data that allow the fulfillment of the requirement to keep reports for the duration of the corresponding work relationship with the whistleblower.
Recipients	The communication of the data is necessary to the IORP and, if required, to competent authorities. This data may also be communicated, in whole or in part, to the whistleblower in the context of a feedback and follow-up of the procedure, provided that this communication does not jeopardize the confidentiality of the person concerned by the report or unless there are legal exceptions.	

Annex 2: Contact information for the whistleblowing officer and internal reporting channels

1. Contact information for the whistleblowing officer

"Priority" whistleblowing officer
Younity Corinne Merla Compliance Officer
"Back up" whistleblowing officer when the "priority" whistleblowing officer is not entitled to act (see point 4, last paragraph of the procedure)
Els De Jaeger Chairman of the Board of Directors of Towers Watson LifeSight OFP

2. Internal reporting channels

Priority channel	
Email	corinne.merla@younity.be[4]
Postal address[5]	Younity, to the attention of Me Corinne Merla, Boulevard du Souverain 36/8, 1170 Brussels, Belgium[6].
phone	+32 2 880 77 88
"Back-up" channel when the priority channel is not entitled to act (see point 4, last paragraph of the procedure)	
Email	els.de.jaeger@wtwco.com
postal address	Willis Towers Watson, to the attention of Mrs. Els De Jaeger, Da Vincilaan 5, Building Caprese, 1930 Zaventem, Belgium.
phone	+32 2 678 15 78

[4] We remind you that the sender usually has the possibility to activate the "private" option in his email.
[5] Please indicate "Confidential" on the envelope.

Annex 3: History of the policy

Date of change	Version	Changes	Date of approval
N/A	1.0	First version	29 December 2020
9 November 2021	1.1	- Signed version	9 November 2021
17 March 2023	1.2	- changes following Belgian whistleblowing law of 28 November 2022	17 March 2023