

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

WHISTLEBLOWER POLICY SMULDERS GROUP

1 Whistleblower user policy – short guide

The whistleblower arrangement is the process that allows you to report a possible breach or serious integrity concern in a work-related context in a safe way. This short guide sets out the policy in clear language, so you can quickly see what you can report, how to report it, what happens next and what protection you may expect.

Important: this is only a summary. The full policy contains the complete rules and always prevails.

Please note: some rules differ depending on the country where your entity is located. That is why you will also find brief country-specific notes below. The full policy also contains the relevant reporting channels, email addresses and telephone numbers.

- **Who can report?** Employees, former employees, applicants, agency workers, interns, freelancers, suppliers, contractors, shareholders and others who obtained information about a possible breach through their work.
- **What can you report?** Possible breaches of law, fraud, corruption, safety issues, privacy issues, environmental harm, financial irregularities and other serious integrity concerns.
- **What is usually not covered by this policy?** Personal complaints about cooperation, pay, employment terms or workplace conflicts. These usually follow HR or grievance procedures.
- **Do you need proof?** No. You do not have to prove anything, but you must have honest and reasonable grounds to think something is wrong.
- **How can you report?** Verbally or in writing, for example through an internal reporting channel, by email, by phone, in a meeting or – where legally possible – externally to a competent authority.
- **Can you choose the reporting channel yourself?** Yes. In principle, you may choose the channel that best fits your situation and the applicable rules, for example an internal or – where legally possible – an external channel.
- **Can you report anonymously?** Yes. Please bear in mind that anonymous reporting may make follow-up more difficult.
- **What should you include in your report?** Describe as clearly as possible what happened, who is involved, where and when it happened, and what information or documents you have about it.
- **Will your report remain confidential?** Yes. Your identity and the information in your report will be handled confidentially. Only the people who need to receive, assess or follow up your report will have access. Your identity will only be shared if this is legally required or if you expressly agree.
- **What happens after you report?** You will normally receive an acknowledgement of receipt within 7 days. After that, it will be assessed whether an investigation should follow. The relevant internal persons and, where necessary, the CKI (Complaints Committee for Infringements) may also be involved. You will usually receive feedback within 3 months on the follow-up or the next steps.
- **Are you protected?** Yes. If you report in line with the applicable rules and have reasonable grounds to think the information is correct, you should not in principle fear retaliation. Dismissal, bullying, disadvantage or other negative consequences because you reported are prohibited. The exact conditions differ by country.
- **Please note differences per country** The main points are briefly summarised below. The full policy always applies for the complete rules.

1.1 Brief country-specific notes

United Kingdom: a different legal framework applies than in the EU.

France: additional conditions apply for protection.

The Netherlands: not every personal complaint relating to the work environment qualifies as a misconduct report.

Belgium and Poland: local rules may differ on scope, procedure and follow-up.

For the full and concrete rules, reporting channels, email addresses, telephone numbers and country-specific details, the full policy always applies.

If you are unsure whether something falls under this policy, it is better to raise your concern or ask for advice through the available channels. Always consult the full policy for the complete and concrete framework, the correct reporting channels, the applicable country-specific rules and all relevant email addresses and telephone numbers.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

2 Introduction

The code of conduct of SMULDERS GROUP NV (hereinafter referred to as 'Smulders') contains core values, standards, and rules for the entire company, which must be respected in our relationships with all our contacts: customers, suppliers, government bodies, shareholders, and employees.

Smulders attaches immense importance to openness, integrity and compliance with laws and regulations. Employees and other stakeholders must be able to report possible violations safely and without fear of negative consequences.

This whistleblower policy describes how reports can be made, how they are managed and what protection whistleblowers may expect. We also refer here to the "Whistleblower User Policy", which briefly and concisely outlines the common thread of the guideline.

It specifies:

- **who** can report
- the **domains** about which one can report.
- **with whom** (channels) and **the methods by which** one can report
- the **protection** that whistleblowers receive
- **the follow-up** that will be given to it.

Smulders does not expect an individual whistleblower to be able to prove that an allegation is justified. However, he/she must be able to demonstrate that there are sufficient grounds to assume that something is wrong.

The organisation of the internal reporting channel, the procedures to be followed for internal reporting and the follow-up of reports are set up after consultation with the social partners.

3 Definitions

CKI: Complaints Committee for Infringements. This is a committee consisting of three people (including a chairman) within the Smulders Group, appointed to manage reports of suspected infringements/misconduct (hereinafter referred to as "CKI").

Data subject: a natural person (e.g. a colleague) or legal entity (e.g. a company) who is named in the report or disclosure as the person to whom the breach is attributed or with whom that person is associated.

Facilitator: a natural person who assists a whistleblower in the reporting process and whose assistance must be confidential.

Information about infringements: information, including reasonable suspicions, about actual or potential infringements that have occurred or are highly likely to occur, as well as attempts to conceal such infringements.

Report manager: the impartial person or service authorised to follow up on reports of breaches, maintain communication with the whistleblower, request additional information from them, if necessary, provide them with feedback and, where applicable, receive and handle reports. For Smulders that is the Compliance Officer.

Retaliation: any direct or indirect action or omission in response to an internal or external report or disclosure, which results or may result in unjustified disadvantage to the whistleblower.

Violation: actions or omissions that:

- are unlawful and relate to the areas listed in Article 4 "Scope", or
- contravene the purpose or application of the regulations falling within the areas of application listed in Article 4.

Whistleblower: a natural person who, in the context of his or her work-related activities, reports or discloses information about breaches verbally or in writing. A work-related activity or context refers to current or former professional activities in the private sector through which, regardless of the nature of those activities, persons

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

may obtain information about breaches and where those persons may face retaliation if they report such information.

The whistleblower may be a(n):

- employee
- former employee
- job applicant
- freelancer/consultant/self-employed service provider
- volunteer
- (un)paid intern
- temporary worker (seconded)
- (employee at a) client
- supplier
- (sub)contractor and/or their employees
- shareholder or
- a person who belongs to the administrative, management or supervisory body of a company, who has obtained information in a professional context about a possible breach that he/she wishes to report.

4 Scope

The scheme distinguishes between social and business integrity. Below is a list of domains to which a report may relate, in accordance with the EU Directive and supplemented with local legislative deviations for Belgium, the Netherlands, the United Kingdom and Poland.

4.1 Social integrity

This category includes undesirable behaviour such as bullying, discrimination, violence, and inappropriate behaviour. These **do not** fall within the scope of whistleblower legislation but are subject to other internal procedures.

- For Belgium see: [R-HRM-IEM-035 Arbeidsreglement Iemants/R-HRM-SPB-044 Arbeidsreglement Smulders Projects Belgium NL/R-HRM-WIL-040 Arbeidsreglement Willems](#)
- For the Netherlands – Vlissingen - see: R-HRM-SPN-002 'Guide for Personnel (Personeelshandboek)'
- For the Netherlands – Schiedam – see: Integriteitsbeleid 2020
- For Poland see: [P-HRA-SPP-002 Escalation Ladder.docx](#)
- For the UK see: R-HRA-SPU-021 Employee Handbook and [R-HRA-SPU-001 Anti-Bullying and Harassment policy](#)
- For France: social integrity (bullying, discrimination, violence, inappropriate behavior/harassment) falls outside the scope of this whistleblowers policy and should be reported via the local HR and psychosocial risk prevention procedures (including “harcèlement”).

4.2 Business integrity

Violations of business integrity, as further specified below, on the other hand, concern, among other things, the handling of confidential information, equipment and goods, health and safety, and the nature of contacts with (potential) customers and suppliers. It also concerns breaches of integrity relating to accounting, financial, banking, audit, bribery, and competition matters.

The difference between the two is that in the case of socially undesirable behaviour, there is often a directly identifiable complainant and defendant between whom the undesirable behaviour occurs, while business integrity issues can be identified and discussed without the whistleblower (e.g. as a victim) being directly involved. In practice, the distinction between social and business integrity is not always clear. As a guideline, undesirable behaviour is primarily directed against an individual, while other integrity violations are more likely to be directed against (the interests of) one's own organisation, external organisations, or society as a whole.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

4.3 DIRECTIVE 2019/1937 - European, Belgian, Dutch, and Polish law

The following domains apply to all Belgian, Dutch, and Polish entities of the Smulders Group. These concern business integrity violations that constitute a breach of EU law or its national implementation (1-15):

1. Public procurement.
2. Financial services, products and markets, prevention of money laundering and terrorist financing.
3. Product safety and product conformity.
4. Transport safety.
5. Environmental protection.
6. Radiation protection and nuclear safety.
7. Food and feed safety, animal health, and animal welfare.
8. Public health.
9. Consumer protection.
10. Protection of privacy and personal data, and security of network and information systems.
11. Infringements relating to the internal market of the European Union, such as infringements of state aid and competition rules: anti-competitive behaviour and agreements, abuse of pricing, abuse of dominant position, etc.
12. Tax fraud.
13. Combating social fraud.
14. Infringements affecting the financial interests of the Union.

For all entities (including the UK) within the EIFFAGE GROUP, reporting is also possible for the following domains:

Infringements concerning :

15. Human rights and fundamental freedoms.
16. Health and safety of persons.
17. Environmental protection, as prescribed by the Act of 27 March 2017, known as the 'Loi sur le devoir de vigilance' (Loi n° 2017-399) concerning the duty of care of parent companies and contractors.
18. Non-compliance with the EIFFAGE Group's Code of Conduct, in particular violations of the prohibition of corruption, bribery, or influence peddling, as well as any other unethical or illegal behaviour.
19. Criminal offences, violations.
20. Threats to or damage to the public interest.
21. A violation (or an attempt to conceal a violation) of Union law, an international commitment ratified or approved by France, a unilateral act of an international organisation based on such a commitment, European Union law, the law, or regulations.

4.4 Country- specific additions or deviations

4.4.1 The Netherlands

The domains under 4.3 also apply to the Netherlands, but the term misconduct (“**misstand**”) is used, when the public interest is at stake. A report may relate to:

- (threat) to danger to personal safety.
- (threat) to danger to public health.
- (threat) to serious environmental damage.
- (threat) to undermining the proper functioning of a company or public service.
- violation of internal rules that contain a legal obligation.

The Netherlands does not deviate from the EU domain list (and the EIFFAGE domains) but applies a broader social assessment.

4.4.2 United Kingdom (UK) — PIDA categories

EU Directive 2019/1937 does **not** bind the United Kingdom. Whistleblower protection in the UK is governed by the Public Interest Disclosure Act 1998 (PIDA), as incorporated into the Employment Rights Act 1996. Under this framework, employees are protected where they make a ‘protected disclosure’ within the meaning of the Employment Rights Act 1996 and reasonably believe that the disclosure is made in the public interest.

4.4.2.1 Qualifying Disclosures

Certain disclosures are prescribed by law as “qualifying disclosures.” A “qualifying disclosure” means a disclosure of information that the Employee genuinely and reasonably believes is in the public interest and shows that the Company has committed a “relevant failure” by:

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

- committing a criminal offence.
- failing to comply with a legal obligation.
- a miscarriage of justice.
- endangering the health and safety of an individual.
- environmental damage
- sexual harassment (as defined in section 26(2) of the Equality Act 2010); or
- concealing any information relating to the above.

Any form of “wrongdoing” that potentially falls within the above categories, regardless of the sector, can be reported.

These acts can be in the past, present or future, so that, for example, a disclosure qualifies if it relates to environmental damage that has happened, is happening, or is likely to happen. The Company will take any concerns that you may raise relating to the above matters very seriously. The employee has no responsibility for investigating the matter - it is the Company's responsibility to ensure that an investigation takes place.

4.4.2.2 Protected disclosures (UK only)

A qualifying disclosure will be regarded as a protected disclosure under the Public Interest Disclosure Act 1998 (PIDA) and the Employment Rights Act 1996 where the employee:

- reasonably believes that the information disclosed is substantially true and is made in the public interest; and
- makes the disclosure through an appropriate reporting route, such as:
 - an internal reporting channel operated by the company.
 - an external disclosure to a relevant prescribed person acting within their regulatory remit; or
 - – in limited circumstances-, a wider or public disclosure, where the statutory conditions for such disclosure are met.

Where a disclosure qualifies as a protected disclosure, the employee is legally protected against dismissal, detriment, or any other form of retaliation because of having made the disclosure.

4.4.2.3 Whistleblowing versus personal employment matters (UK only)

Matters relating exclusively to an individual's personal employment situation, such as personal complaints regarding salary, working conditions, interpersonal conflicts, or management decisions, do not normally fall under “whistleblowing” and should be reported via the designated complaints procedure or HR procedure, unless the matter also affects a broader public interest or falls within the scope of a qualifying report as described above.

When a matter has both a personal impact and serves a broader public interest, it may fall within the scope of this whistleblower policy.

All forms of ‘wrongdoing’ that potentially fall within the above categories, regardless of sector, may be reported.

4.4.3 France

For France, the French whistleblowers framework (“lanceur d’alerte” Law n° 2016-1691 as amended in 2022) includes the requirement that the whistleblower acts in good faith and without any direct personal financial gain.

5 Submitting a report and follow-up steps

A. With whom?

A whistleblower has several channels at their disposal to report a violation.

- Whistleblowers are encouraged, where appropriate and feasible, to raise concerns internally (e.g. with their manager), as this often allows issues to be addressed quickly and effectively. However, internal reporting is not mandatory, and whistleblowers may report directly through internal or external reporting channels, in accordance with the applicable legal framework.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

- Where a whistleblower chooses to raise a concern with their manager and circumstances do not allow this, or the manager does not respond adequately, the whistleblower may submit a (suspected) breach to the hierarchical superior of their manager.
- The whistleblower also always has the right to consult their employee representatives or trade unions, and they will remain protected against unjustified adverse measures as a result of these consultations.
- Where the whistleblower considers that, for any reason, they cannot turn to the persons referred to above, they may make an internal report to the CKI.
An internal report is a report of a breach within a legal entity (the company) by providing verbal or written information about breaches via the internal reporting channel, the procedure for which is described in more detail under Section B, "HOW TO REPORT."
- Whistleblowers may make an external report, either verbally or in writing, via the external reporting channel organized by the competent authority, as further explained under Section 4 E, "SUBMITTING A REPORT VIA THE GOVERNMENT'S EXTERNAL REPORTING CHANNEL". This may be done without prior internal reporting, or after the internal reporting channel has been used, where appropriate and in accordance with applicable law.
- A public report or disclosure of information about breaches is possible only if the strict conditions set out in Section 6, "DISCLOSURE OF A VIOLATION IN EXCEPTIONAL CIRCUMSTANCES", are met.

The whistleblower has the option of submitting an anonymous report, and such reports will be received and handled with due care.

Whistleblowers should be aware that anonymous reporting may involve certain practical limitations, including:

- it may be more difficult to seek clarification or additional information where needed; and
- it may limit the ability of the Company to provide individual feedback or personalised protection against possible reprisals.

These limitations will not in themselves result in the report being disregarded.

B. How to report?

Internal reports can be submitted verbally or in writing via:

- a) e-mail ethics@smulders.com
- b) web application <https://eiffage.integrityline.org>
- c) telephone/voice messaging system:

- For Belgium:

Mrs. Katy Rijnders: Mob.: +32 (0) 478 506 428

- For the Netherlands - Vlissingen:

Mr. Sander Meijers: Mob.: +31(0) 6 15426527

- For the Netherlands – Schiedam

Mr. Paul Wenting: Mob.: +31(0) 6 51370674

- For the UK:

Mrs. Amanda Young: Mob.: +44 7387 411624

- For Poland:

Mrs. Katarzyna Dendewicz: Mob: +48 606252937

- For France:

Mrs. Samia Ben Belaïd: Tel. + 33 610 166 307

- d) physical meeting within a reasonable period of time:

- For Belgium:

Mrs. Katy Rijnders: +32 478 506 428 Katy.rijnders@smulders.com

- For the Netherlands - Vlissingen:

Mr. Sander Meijers: Sander.Meijers@smulders.com Mob.: +31(0) 6 15426527

- For the Netherlands – Schiedam

Mr. Paul Wenting: paul.wenting@smulders-hsm.com Mob.: +31(0) 6 51370674

- For the UK:

Mrs. Amanda Young: Amanda.Young@smulders.com Mob.: +44 7387 411624

- For Poland:

Mrs. Katarzyna Dendewicz: Katarzyna.Dendewicz@smulders.com Mob: +48 606252937

- For France:

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

Samia Ben Belaïd: Samia.Ben.Belaid@smulders.com Tel. +33 610 166 307

A report must contain at least:

- The name, address, position, and contact details of the whistleblower if they do not wish to make an anonymous report.
- The date of the report.
- A detailed description of the (alleged) breach, such as
 - a description of the (alleged) infringement.
 - any attachments (documentation or supporting evidence).
 - the identification of the possible person(s) or departments of the company involved.
 - where the infringement occurred.
 - when the infringement took place.
 - how and when the whistleblower noticed the breach or was informed of it.
 - your relationship with the company (employee, freelancer, supplier, shareholder, etc.), unless the whistleblower is making an anonymous report.
 - the impact of the incident (on the company, on the public interest, etc.)
 - and any other relevant information regarding the (alleged) breach

Ad b) Online reports can always be submitted via the EIFFAGE GROUP's secure internal reporting channel: <https://eiffage.integrityline.org>

Consult the FAQ on this site for practical questions about submitting and following up on reports by EIFFAGE alert managers.

The internal reporting channel is hosted by EQS and is an encrypted platform with data storage within the European Union.

C. Admissibility and preliminary investigation

- a) The report manager will always confirm receipt of the written report to the whistleblower within seven (7) days.
 - The report manager will first check whether the report is admissible and will make an initial assessment. The primary purpose of this assessment is to evaluate the nature, reliability and accuracy of the information provided.
 - Based on this assessment, the report manager may decide that the report is inadmissible, in which case he must inform the whistleblower in writing of the reason for rejection, or that he will conduct a further preliminary investigation.
- b) If a preliminary investigation is initiated and the report manager considers that further investigation is necessary, an anonymised opinion will be submitted to the CKI after completion and with the consent of the whistleblower. This opinion will set out the reasons for further investigation and include an initial action plan.
- c) If the preliminary investigation reveals that the report is deliberately false, the file will be forwarded to Smulders involved HR Director for further action.

D. Investigation

- a) The CKI will decide, on the basis of the aforementioned advice, whether and with which investigation committee the investigation should be carried out: either only by the report manager, or the complete CKI and/or supplemented in each case by internal or external experts, or an external party, supplemented where appropriate by internal (staff) member(s).
- b) The whistleblower will also be informed in writing that a thorough investigation is being launched.
- c) The investigation committee will conduct the investigation within a reasonable timeframe, considering the nature and complexity of the report.
Where possible, feedback on the follow-up, the measures planned or taken and the reasons for that follow-up will be provided typically within three months after confirmation of receipt has been sent to the whistleblower.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

- d) During the investigation and therefore also after the initial three-month period, the whistleblower will receive general information about the progress of the investigation and the outcome, unless the whistleblower does not wish this or it is detrimental to the whistleblower or the investigation, or unless there are other valid reasons for not informing the whistleblower.
- e) Final report.

The final report includes the following steps:

- a) The report manager or investigation committee reports its findings in writing to the Chairman of the CKI, who decides what action should be taken.
- b) The report manager informs the whistleblower that the findings of the investigation committee have been sent to the Chairman of the CKI.
- c) The identity of the whistleblower is protected in the final report, unless they have given their written consent to disclose their identity. The identity of the person(s) involved is only included if the investigation of the report has led to demonstrable facts.
- d) If the Chairman of the CKI considers that disciplinary action should be taken, he or she will provide a copy of the final report to the appropriate person in management.

E. Submitting a report via the government's external reporting channel

After first submitting a report via an internal reporting channel, the (anonymous) whistleblower may report a violation via an external government reporting channel if no appropriate measures have been taken via the internal procedure. The whistleblower may also submit a report directly via the external government reporting channel.

The following contact points are officially recognized national ombudsman services:

Please note there are also multiple competent authorities per country for each topic/domain (financial services, privacy, healthcare, consumer law, etc.). The central bodies listed below assist whistleblowers with referrals to the appropriate authority or serve as a safety net.

Belgium – Federal Ombudsman

This authority provides an overview of the competent authorities, depending on the type of infringement.

- contact@federaalombudsman.be
- +32 2 289 27 27
- Leuvenseweg 48 bus 6, 1000 Brussels

Netherlands – Huis voor Klokkenluiders (House for Whistleblowers – Refer to the competent authority)

- contact@huisvoorklokkenluiders.nl
- +31(0)88 13310 00
- Visiting address: Muzenstraat 89, 2511 WB The Hague.
- Postal address: PO Box 85680, 2508 CJ The Hague

Poland – Commissioner for Human Rights (Rzecznik Praw Obywatelskich, RPO)

The Ombudsman receives reports, conducts an initial assessment, and refers them to the competent public authority.

- biurorzecznika@brpo.gov.pl
- 800 676 676
- Al. Solidarności 77, 00 090 Warsaw

France – Défenseur des droits (guidance/referral to the competent authority)

The Défenseur des droits informs whistleblowers about their rights, helps identify the correct external reporting route and may refer reports to the competent authority depending (“autorité compétente”) on the subject matter.

- via an online form (Défenseur des droits website)
- +33 (0)9 69 39 00 00 (Mon–Fri, during office hours; cost of a local call)
- Défenseur des droits – Libre réponse 71120, 75342 Paris CEDEX 07

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

France – CNIL (competent authority: privacy/data protection)

- depotplainte@cnil.fr
- +33 (0)1 53 73 22 22
- 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07

United Kingdom – Prescribed Persons

In the United Kingdom, external reports are made to so-called “prescribed persons.” These are government-appointed supervisory bodies authorized to receive reports within their specific domain. The United Kingdom does not have a central authority that receives or refers reports. The whistleblower is responsible for choosing the appropriate competent authority.

The complete and most up-to-date list of prescribed persons, including their contact details, is available from the UK government:

<https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies>

Examples of common prescribed persons include:

Domain	Organisation	Contact
Telecommunications, media, online safety	Office of Communications (Ofcom)	Tel. 0300 123 3333 / 020 7981 3040; PO Box 1285, Warrington WA1 9GL; www.ofcom.org.uk [gov.uk]
Financial services, markets, conduct	Financial Conduct Authority (FCA)	Via GOV.UK prescribed list (online reporting) [gov.uk]
Competition law	Competition and Markets Authority (CMA)	Via GOV.UK prescribed list [gov.uk]
Privacy & data protection	Information Commissioner's Office (ICO)	Via GOV.UK prescribed list; www.ico.org.uk [gov.uk]
Health & safety at work	Health and Safety Executive (HSE)	Via GOV.UK prescribed list; www.hse.gov.uk [gov.uk]
Environment & pollution	Environment Agency (England)	Via GOV.UK prescribed list [gov.uk]
Taxation, customs, national insurance	HM Revenue & Customs (HMRC)	Via GOV.UK prescribed list [gov.uk]
Serious or complex fraud, bribery & corruption	Serious Fraud Office (SFO)	Via GOV.UK prescribed list [gov.uk]
Police conduct	Independent Office for Police Conduct (IOPC)	Via GOV.UK prescribed list [gov.uk]
Company misconduct, insolvency, director fraud	Insolvency Service – Intelligence Team	Via GOV.UK prescribed list [gov.uk]

An up-to-date and complete list of prescribed persons, including their contact details and the matters that may be reported to them, is published by the UK Government and is available at: <https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies>.

The external reporting channel will provide feedback to the whistleblower **within three (3) months** or, in exceptional cases, **six (6) months**, on the planned follow-up or measures taken and the reasons for that follow-up, unless a legal provision prevents this. The external reporting channel will inform the whistleblower of the outcome of the investigations.

The competent authorities may decide that a reported breach is clearly minor or has already been the subject of previous reports on the same facts without any additional new elements, with the result that they close the procedure. The competent authorities shall inform the whistleblower of their decision and the reasons for it.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

When making a disclosure to a prescribed person, the whistleblower should reasonably believe that the information disclosed is substantially true and that the prescribed person is the appropriate body to receive the disclosure in relation to the matter concerned.

6 Disclosure of a violation in exceptional circumstances

An (anonymous) whistleblower who discloses a breach by making information about breaches publicly available (e.g. through the media) is eligible for protection if the following conditions are met:

1. The whistleblower has first made an internal or external report as prescribed under titles b) or c), but no appropriate measures have been taken; or,
2. The whistleblower has reasonable grounds to believe that:
 - the breach may pose an imminent or real danger to the public interest; or
 - in the case of an external report, there is a risk of retaliation, or it is unlikely that the breach will be effectively remedied due to the particular circumstances of the case, for example because evidence may be withheld or destroyed, or an authority may collude with the perpetrator of the breach or be involved in the breach.

7 Guarantees for the position of the whistleblower

A. Conditions for protection

The whistleblower will be protected if they have reasonable grounds to believe that the information is accurate and falls within the scope of application. Anonymous whistleblowers who are later identified may also enjoy protection.

Not only the whistleblower, but also facilitators, family members or legal entities associated with the whistleblower may be protected against reprisals.

The following persons and legal entities are protected if they have reasonable grounds to believe that the whistleblower is covered by the protection condition:

- Facilitators.
- Third parties associated with the whistleblowers who may be subject to retaliation in a work-related context, such as colleagues or family members of the whistleblowers.
- Legal entities owned by the whistleblowers, for which the whistleblowers work or with which the whistleblowers are otherwise connected in a work-related context.

B. Confidentiality

The report manager, including the authorised staff members responsible for receiving and following up on reports, shall keep the identity of the whistleblower confidential. The reporting manager is also designated for the sake of confidentiality in the handling of the case and the identity of the whistleblower, and for the sake of independence to avoid conflicts of interest. More specifically, during the handling of the report, it is prohibited to disclose the identity of the whistleblower or any information that could lead to the whistleblower's identity being discovered. The obligation of confidentiality also applies if an anonymous whistleblower can still be identified directly or indirectly through other information.

The reporting manager may only disclose the identity of the whistleblower:

- if the whistleblower gives its free and explicit (written) consent; or
- if the whistleblower deliberately breaches confidentiality.

Confidentiality of identity will not apply if mandatory legislation requires disclosure in the context of investigations by national authorities or legal proceedings. The competent authority will inform the whistleblowers in advance of the reasons for the disclosure unless this would jeopardise the investigations or legal proceedings.

Anyone directly or indirectly involved in the handling of a report of a (suspected) breach is obliged to maintain confidentiality about everything entrusted to him/her or disclosed to him/her in connection with this (such as the report, the preliminary investigation and the investigation itself) vis-à-vis anyone who is not authorised to take cognisance of this and insofar as these obligations follow from the nature of the matter.

The internal reporting channel for receiving reports is designed, structured and managed in such a way as to securely protect the confidentiality of the identity of the whistleblower and any third parties mentioned in the report, and to which unauthorised personnel have no access.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

C. Prevention of reprisals, such as sanctions or unfair treatment

Retaliation is any direct or indirect act or omission in a work-related context to the detriment of a whistleblower following an internal or external report or disclosure, which leads or may lead to unjustified disadvantage to the whistleblower. Any form of retaliation, including threats and attempts at retaliation, is prohibited and includes in particular:

- suspension, temporary removal from duty, dismissal, or similar measures.
- demotion or refusal of promotion.
- transfer of duties, change of workplace location, reduction in salary, change in working hours.
- withholding training.
- negative performance assessment or employment reference.
- imposition or application of a disciplinary measure, reprimand, or other sanction, such as a financial penalty.
- coercion, intimidation, harassment, or exclusion.
- discrimination, unfavourable or unequal treatment.
- failure to convert a temporary employment contract into a permanent employment contract, in the event that the employee had a legitimate expectation that he would be offered permanent employment.
- non-renewal or early termination of a fixed-term employment contract.
- damage, including damage to reputation, particularly on social media, or financial loss, including loss of turnover and loss of income.
- blacklisting based on an informal or formal agreement for an entire sector or industry, because of which the person can no longer find a job in that sector or industry.
- early termination or cancellation of a contract for the supply of goods or services.
- revocation of a licence or permit.
- psychiatric or medical referrals.

Whistleblowers acting in accordance with this policy may make their report without jeopardising their employment status or fearing any other adverse consequences. This implies that they will not be disadvantaged in any way because of this question or report, provided that they act in good faith.

Retaliation against whistleblowers because of a sincere report is considered a serious violation of this whistleblowers policy, the Smulders' Code of Conduct, as well as the EIFFAGE's Code of Conduct, in which case Smulders will take appropriate action to protect the whistleblower and to sanction those responsible for the retaliation.

Whistleblowers who believe they have suffered adverse consequences because of a report must notify the report manager as soon as possible. Victims of reprisals can also submit a substantiated complaint to the federal coordinator, who will initiate an out-of-court protection procedure if he has established reasonable suspicion of reprisals. The federal coordinator who will manage this complaint is the Federal Ombudsman, whose contact details are listed in Section 5, E. SUBMITTING A REPORT VIA THE GOVERNMENT'S EXTERNAL REPORTING CHANNEL.

The federal coordinator will verify with Smulders whether there is reasonable suspicion of retaliation. Smulders will respond to the federal coordinator's request within twenty (20) days.

Statutory protection (UK)

In the United Kingdom, employees who make a protected disclosure are entitled to statutory protection under the Public Interest Disclosure Act 1998 and the Employment Rights Act 1996.

This includes protection against any detriment suffered on the ground that a protected disclosure has been made, as well as protection against automatic unfair dismissal where dismissal occurs principally because of such a disclosure.

8 Abuse of the reporting system

Smulders assumes that whistleblowers will report breaches in good faith. If, upon further investigation, the report manager cannot find confirmation for certain reports or if they prove to be unfounded, no measures will be taken against whistleblowers who have expressed their concerns in good faith.

However, Smulders cannot allow whistleblowers to deliberately submit reports that they know or should know to be false. Smulders will appropriately sanction deliberately false reports in accordance with the sanctions

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

prescribed in the employment regulations. Whistleblowers acting in bad faith may be held liable for any damage suffered by anyone because of false reports.

Whistleblowers who have deliberately reported or disclosed false information may be prosecuted for defamation or damage to the reputation of individuals.

9 Processing of personal data and your rights

Smulders is the controller of personal data in the implementation of this reporting scheme. For UK-based whistleblowers and processing activities carried out in the United Kingdom, references in this policy to the GDPR shall be understood as references to the UK GDPR, as supplemented by the Data Protection Act 2018. This implies that both the whistleblower and the person concerned can contact Smulders to exercise their right to information, access, correction, portability, and deletion of data, subject to the following restrictions:

- The data subject (the subject of the reported breach) has no right to access the identity of the whistleblower or that of third parties (or elements that could enable their identification), unless with their consent or in the event of a false report or defamatory allegation by the whistleblower or false testimony by a third party.
- Nor does the whistleblower have the right to access the personal data of the accused or of a third party, unless an investigation reveals that the accused has wrongfully suspected the whistleblower (e.g. by claiming that the whistleblower was himself involved in the malpractice he reported) or when third parties act in bad faith (e.g. false testimony).
- The personal data of the parties involved will not be deleted as long as the internal and/or external (police/judicial/administrative) investigation is ongoing.
- The personal data will not be sent to third countries that do not provide an adequate level of protection for your personal data.

During the reporting procedure, in addition to the facts, the name, position and contact details of the whistleblower and the accused will also be processed.

The processing of this personal data is necessary within the framework of the Act of 28 November 2022 on the protection of whistleblowers who report breaches of Union or national law within a legal entity in the private sector (Art. 6, §1, c) GDPR).

The transfer of a report to a processor (a service provider such as a cloud storage provider or tool for managing reports) may be based on the legitimate interests of Smulders to process this data efficiently for the purposes of managing reports, ensuring anonymity, access management, etc. (Art. 6, §1, f) GDPR). If you make a report by means of a voice recording, this will be done based on your consent (Art. 6, §1, a) GDPR).

The whistleblower can always contact Smulders at privacy@smulders.com if he/she should have any further questions about the safeguards taken to protect its personal data and about the processing of its personal data in the context of the reporting scheme, or to request its right of access to, correction or transferability of data, or deletion of its personal data, insofar as the exercise of these rights falls within the legal conditions.

If, after contacting Smulders, the whistleblower still wishes to lodge a complaint regarding the processing of your personal data, the whistleblower can contact the competent supervisory authority, namely the Data Protection Authority.

The government body responsible for the external reporting channel acts as the controller. This means that, in the case of external reports, you can contact the government to exercise your rights.

The competent authorities and the Federal Institute for the Protection and Promotion of Human Rights (accessible via this link: <https://federaalinstituutmensenenrechten.be/nl/contact> or via [info\[at\]firm-ifdh.be](mailto:info[at]firm-ifdh.be)) will inform and advise you on support measures, such as:

- information and advice on the available remedies and procedures offering protection against reprisals, as well as on the rights of the person concerned.
- technical advice regarding authorities involved in the protection of the whistleblower.
- legal assistance and financial assistance in the context of legal proceedings.
- technical, psychological, media-related, and social support.

R-HRA-GR-003	Whistleblowers – Klokkenluiders policy		Rev.:	1-0
			Date:	13/05/2026
Author:	Katy Rijnders	Validated by:	Joren Daenen, Inge Hendrix, Carine Delava, Katarzyna Dendewicz, Amanda Young, Jantine Stins	

10 Retention period

The personal data processed in the context of the reporting scheme will not be retained for longer than is necessary for the internal and/or external (police/judicial/administrative) investigation. In the event of police, administrative, judicial, or disciplinary proceedings, the data will be archived after the expiry of the applicable limitation period or appeal period or retained for up to two (2) months thereafter.

11 Sanctions

The infringements listed in Section 4. Scope' of this policy concerning the reporting procedure and established in the final result of the investigation of a complaint via this reporting procedure may give rise to sanctions (including a warning or dismissal for urgent reasons) as described in the employment regulations or the employment contract.

In addition to these labour law sanctions, the person concerned or the whistleblower may, depending on the nature of the violation and the applicable legislation, incur additional sanctions, such as criminal sanctions and damages.

12 Management cooperation

To ensure that this reporting procedure is properly embedded, management will undertake the following activities:

- Ensure that this procedure is available and known to all employees.
- Take all matters relating to reports of integrity violations very seriously, take timely action and guarantee confidentiality and care.

13 Other provisions

This scheme will be evaluated within two (2) years of its entry into force.
In cases not covered by this policy, the Chairman of the CKI shall decide.