



Whistleblowing Charter

November 2025

INTEGRITY AND COMPLIANCE ARE AT THE HEART OF IDVERDE GROUP'S POLICY.

The values set out in *idverde's* Code of Ethics and Integrity Guidelines are part of the Group's reputation and guarantee the safety of its employees and the trust of its customers and partners. These values are fundamental, and binding on everyone.

Transparency and ethical vigilance are the safeguards of our corporate integrity. Everyone is therefore encouraged to raise concerns or report any situation that appears to conflict with these values. Similarly, line managers are expected to promote open dialogue with their teams and facilitate the reporting of concerns so that appropriate action can be taken promptly.

If reporting through the normal hierarchical channels is not possible or desired, the confidential and secure whistleblowing reporting system set up by *idverde* can be used.

Reporting a situation that appears to conflict with the ethical values of the *idverde's* Group is entirely voluntary and should result from a personal and considered decision. However, in making this decision, a potential whistleblower is encouraged to reflect on the role their report may play in protecting the company and its employees.

This charter sets out the procedures and safeguards applicable to the whistleblowing system.

This charter may be updated from time to time to reflect legal or organisational developments. The latest version will be made available on the *idverde* Group website or on request.

1. Who can use the whistleblowing system and for what purposes?

1.1 Who can report?

The internal reporting system can be used by:

- employees, trainees, former employees and applicants (if the information was obtained during previous employment or during the recruitment process).
- external and temporary employees (including secondees, contractors, agents, and representatives).
- shareholders, associates and holders of voting rights in *idverde* Group companies.
- members of *idverde's* administrative, management or supervisory bodies.
- *idverde's* business partners (such as, subcontractors, suppliers and customers) and their relevant staff or representatives.

To qualify as a “whistleblower”, the individual must also:

- Have personal knowledge of the reported information if it was not obtained professionally.
- Act in good faith and have reasonable grounds to believe that the reported information was true at the time of reporting.
- Act without seeking direct personal interest or financial gain.

1.2 What can be reported?

Reports may concern actual or suspected:

- Criminal offences or misconduct (e.g., corruption, bribery, influence peddling, anti-competitive practices, human rights abuses, discrimination, harassment),
- Violations or concealment of violations of laws, regulations, EU law, or international rules,
- Threats or damage to the public interest (e.g., environmental damage, health and safety of individuals),
- Violations of idverde's Integrity Guidelines or Code of Ethics.

Reports must not concern information disclosure that is expressly prohibited by law, including but not limited to: national defence secrecy, medical secrecy, secrecy of judicial deliberations, secrecy of judicial inquiries or investigations, or legal professional privilege.

2. How to make a report

idverde encourages the individuals mentioned in Section 1.1 to use the internal reporting system but reminds them that doing so is entirely voluntary, and no adverse consequences will result from choosing not to report.

Important: Misuse or reports made in bad faith (e.g., making false accusations) may lead to disciplinary and/or legal action.

2.1 Reporting options

Reports may be submitted:

- via the **idverde Integrity Line** platform (*accessible 24/7 and available in multiple languages*)
 - **Online:** <https://idverde.integrityline.com>
 - **Telephone:** dial your organisation's specific number and enter the 4-digit PIN: **9013**

idverde Denmark	+45 78 15 23 29
idverde France	+33 1 87 21 22 91
idverde Germany	+49 30 9925 7146
idverde Luxembourg	+352 27 860 540
idverde Netherlands	+31 20 323 23 45
idverde Switzerland	+41 43 551 02 35
idverde United Kingdom	+44 20 3885 0064
- directly to the **Group Legal and Compliance Director** (the "Referent"):
 - **Email:** integrite@idverde.com
 - **Postal address:** Armorica Lux S.à.r.l. - idverde Group
21 rue Glesener, L-1631, Luxembourg

Subject to the applicable legal requirements in the relevant jurisdiction, the whistleblower may also be entitled to report to external designated authorities under certain conditions. Individuals are encouraged to consult the national framework and seek legal advice where appropriate.

2.2 How to submit a report

Reports may be submitted in writing or orally.

1. Written reports

Written reports should include the following elements:

- The words "*confidential*" and "*report*" in the subject line.
- The date, time, and location of the incident(s), if known.
- A precise and detailed description of the facts and the circumstances in which the whistleblower became aware of them.

The whistleblower may choose to:

- disclose their identity and provide contact information, or
- submit an anonymous report.

While *idverde* encourages whistleblowers to identify themselves to support follow-up, anonymous reports will be handled with the same diligence and confidentiality. However, anonymity may limit our ability to obtain further information or provide updates.

2. Oral reports

Whistleblowers who wish to make an oral report must contact the Referent, who will organise an interview within twenty (20) working days of the request.

Oral reports will be recorded using one of the following methods, with the consent of the whistleblower:

- via a recorded telephone or voice messaging system. The conversation may be recorded on a durable and retrievable medium or transcribed in full.
- via an unrecorded telephone line or voicemail system. A detailed written record of the conversation will be prepared.
- during a videoconference or physical meeting. A recording or a written transcript will be produced.

The whistleblower will have the opportunity to review, correct, and approve the transcript or meeting minutes by signing the final version.

3. How reports are handled

3.1 Receipt of a report

Upon registration of a report, the Referent will acknowledge receipt in writing within seven (7) working days of receipt. This acknowledgement does not imply that the report is deemed admissible or well-founded.

3.2 Admissibility review

The Referent assesses whether the report meets the admissibility criteria, and may request additional information or evidence of eligibility, as referenced in Section 1.1 (unless the report is anonymous).

The whistleblower will be informed of the outcome of the admissibility assessment. If the report is not admissible, the Referent will specify the reason(s) for inadmissibility.

3.3 Investigation and follow-up

Within a reasonable period not exceeding three (3) months from the date of acknowledgment of receipt - or, where no acknowledgment has been issued, from the expiry of a seven (7) working day period following submission of the report - the Referent shall provide the whistleblower with feedback. Such feedback may include a summary of the actions taken or planned in response to the report, subject to applicable legal provisions and any confidentiality obligations.

The Referent may involve internal staff members, within the scope of their duties, or establish an ad hoc ethics committee to support the investigation. Where necessary, the Referent may engage external consultants or advisors. Anyone involved in handling the report shall be bound by a duty of confidentiality.

3.4 Closure of the report

A report - whether submitted anonymously or not - will be closed in any of the following situations:

- It is deemed inadmissible based on the conditions set out in Sections 1.1 and 1.2.
- The reported facts are found to be inaccurate, unfounded, or the report is no longer relevant.
- The investigations have been completed.

Unless the report was submitted anonymously, the whistleblower will be notified in writing, through their preferred means of communication, of the closure of the case and of the reasons for the decision.

3.5 Retention and destruction of the report file

The retention of data related to a report depends on the nature of the report and its outcome. idverde ensures that all personal data is processed and stored in accordance with applicable data protection laws and statute limitations.

- If a report is found to be inadmissible, all personal data contained in the report will be destroyed or anonymised promptly.
- If the report is deemed admissible:
 - Personal data will be retained in an active database only for as long as necessary to assess the report, conduct any related investigations, and take appropriate follow-up action.
 - Once a final decision has been made, the data may be archived for a period that is strictly necessary and proportionate to complete any residual follow-up actions, protect the rights of the whistleblower and third parties involved, taking into account the applicable statutes of limitation.
- If legal or disciplinary proceedings are initiated as a result of a report, or against the whistleblower in the case of a malicious or abusive report, the data will be retained until the conclusion of the proceedings, the expiry of any applicable limitation period, or the exhaustion of all remedies, whichever is the later.

4. Confidentiality and data protection

4.1 Confidentiality

All individuals involved in the handling of reports are subject to an obligation of reinforced confidentiality. They must ensure the strict confidentiality of:

- the identity of the whistleblower,
- the identity of any person involved or mentioned in the report, and
- all information collected in connection with the report.

Information related to a report may only be disclosed to third parties if such disclosure is strictly necessary for processing the report.

In such case:

- Information that could reveal the identity of the whistleblower may only be disclosed with their explicit consent. However, such information may be disclosed to judicial authorities if the person responsible for receiving and processing the report is legally obliged to report the facts. In that case, the whistleblower will be informed in writing of the reason for this disclosure, unless doing so would compromise the judicial proceedings.
- All necessary precautions will be taken to ensure that (i) the information is shared only with individuals who have a legitimate need to know, and (ii) those individuals are made aware of their confidentiality obligations.

Information that could identify a person who is the subject of the report may not be disclosed, except to the judicial authorities, and only after the report has been duly assessed and deemed to be well-founded.

4.2 Protection of personal data

Personal data collected in connection with a report and the subsequent internal investigation will be processed by *idverde*. The purpose of this processing is to assess the merits of reports submitted through the professional report system and to determine appropriate actions.

This processing is based on *idverde*'s legitimate interest in ensuring compliance with its internal rules, in particular those set out in the Integrity Guidelines and the Code of Ethics, or to comply with a legal obligation relating to ethics and compliance.

Where necessary, sensitive personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to identify an individual, health data, or data concerning a person's sexual activity or sexual orientation, as well as data relating to offences, convictions, or security measures, may also be processed. Such processing will only occur when necessary for the establishment, exercise, or defence of legal claims.

The personal data processed may include identification details, professional information, and any data derived from the report.

This data may be shared with internal recipients within *idverde* who require access for the purposes of handling the report or conducting the investigation, and with external recipients such as legal advisors, service providers whose involvement is essential to the investigation of the report, or competent authorities who need to be informed of its outcome.

The retention period applicable to this data is set out in Section 3.5 of this charter.

Data subjects have the right to request, in accordance with applicable data protection law (including Regulation (EU) 2016/679 – GDPR):

- access to their personal data
- rectification of inaccurate or incomplete data
- erasure of their data, where applicable
- restriction of processing in specific circumstances; and
- objection to the processing of their personal data, except where such processing is required to comply with a legal obligation.

These rights may be restricted where necessary to protect the rights and freedoms of third parties or the identity of the whistleblower.

Questions or requests to exercise data rights should be addressed to the Referent at: integrite@idverde.com

If a data subject considers that their request has not been handled satisfactorily, they have the right to lodge a complaint with the relevant supervisory authority.

5. Whistleblower protections

Whistleblowers who make a report in good faith and in accordance with this charter shall benefit from the protection measures set out below.

No whistleblower shall be subject to retaliation, threats, or attempts to retaliate in any form, in relation to their whistleblowing. This includes, but is not limited to, dismissal, suspension, or lay-off; disciplinary action, demotion or denial of promotion; restriction from training or professional development; discrimination or any form of disadvantageous or unfair treatment; non-renewal or early termination of an employment contract; early termination or cancellation of a contract for goods or services.

Anyone found to have engaged in retaliatory conduct may be subject to disciplinary or legal action.

The whistleblower shall not incur civil liability for damages resulting from a report or public disclosure, provided that the whistleblower had reasonable grounds to believe that the disclosure was necessary to protect the relevant interest.

The whistleblower shall not be held criminally liable for breaching a legally protected secret if the disclosure was both necessary and proportionate to protect the relevant interest and was made in accordance with applicable law.

The measures for protection set out in this Section shall also apply, where relevant, to:

- Facilitators - natural persons or any non-profit legal entities (e.g. trade unions, associations) who assist the whistleblower.
- Third persons who are connected with the whistleblower and who could suffer retaliation in work-related context, such as colleagues or relatives of the whistleblower.
- Legal entities that the whistleblower owns, works for or are otherwise connected with in a work-related context.

idverde
21 rue Glesener
L1631 Luxembourg