

# Baker Tilly in Luxembourg

## Whistleblowing channel guidelines

### Introduction: what is whistleblowing, and why is it important?

Baker Tilly in Luxembourg consists of the following entities:

- Baker Tilly Luxembourg Experts-Comptables S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Corporate Services S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Advisory S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Training S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Luxembourg Innovation S.A., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Interaudit S.à r.l., 37, Boulevard des Scillas, L-2529 Howald, Luxembourg,
- Baker Tilly Audit & Assurance s.à r.l., 2, rue Peterelchen, L-2370 Howald, Luxembourg,
- Fibetrust S.à r.l., 45, Boulevard des Scillas, L-2529 Howald, Luxembourg,

(hereinafter referred to as "Baker Tilly") strives to ensure that transparency is combined with a high standard of professional ethics. With this in mind, the Baker Tilly has put in place this internal procedure and an internal whistleblowing channel, giving employees and external stakeholders the opportunity to report in confidence any suspicions of misconduct. As explained in the rest of this document, whistleblowing can be carried out either in confidence or anonymously.

This document is part of our compliance with the Luxembourg law on whistleblowing (Law of 16 May 2023 transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report violations of Union law) as well as legislation on personal data protection (Law of 1 August 2018 organising the National Data Protection Commission and implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals).

### When should a whistleblowing alert be raised?

Our whistleblowing service can be used to report serious risks affecting you, your colleagues or other individuals, as well as the company. Problems reported may include crimes, misconduct, violations or other actions in breach of European or national laws, in a **business context**, such as:

- ✓ **Corruption and financial misconduct;** e.g. bribery, unfair competition, money laundering, fraud, conflict of interest.
- ✓ **Health and safety violations;** e.g. workplace health and safety, product safety, serious discrimination and harassment, all of which are against the law.
- ✓ **Environmental violations;** e.g., illegal treatment of hazardous waste.
- ✓ **Privacy violations;** e.g. misuse of personal data.

Please note that this whistleblowing service is not intended for raising personal grievances relating to your working conditions, performance appraisal or similar concerns. We invite you to discuss your concerns with your manager.

A whistleblower does not need to have conclusive evidence to raise a suspicion. However, deliberate reporting of false or defamatory information will be punishable. Any abuse of the whistleblowing service is a serious offence punishable by disciplinary action.

## How to raise an alert?

Send an anonymous or confidential message via the whistleblowing channel to the whistleblowing team: <https://bakertillylux.integrity-speakingup.com/en/report>. The link is available on our website and the platform can be accessed by scanning the below Qr code:



You can submit your report filling in a form on the website. You can do this from your computer or smartphone. Please refer to the link above for further information on how to use the platform.

If you have followed the above steps to raise an alert but believe that the matter has not been satisfactorily resolved, in accordance with legal obligations and within 3 months, you may report the matter directly to the relevant competent authority. In this case, you can contact the Reporting Office (13, rue Erasme, Centre administratif Werner, L-1468 Luxembourg, Tel: (+352) 247-88564), or by email at the following address: [ods.info@mj.etat.lu](mailto:ods.info@mj.etat.lu) for further information on the relevant competent authority depending on the type of report raised..

## The investigation process

### THE INVESTIGATION TEAM

Access to messages received via the whistleblowing channel is restricted to designated individuals responsible for managing alerts. Their actions are traced in the event log and the handling of alerts is strictly confidential. In line with the above, our organisation has appointed an external and independent consulting firm ('Grant Thornton Advisory') as the 'alert management team' to be primarily responsible for the management of the platform and any reports.

When necessary, experts - 'investigators' - will be called in to the platform to carry out the investigation. These individuals may access the relevant data as you have shared it and are also required to maintain strict confidentiality and/or anonymity.

### **MANAGING RECEIVED MESSAGES**

When a whistleblower alert message is received, the alert management team decides whether to accept or reject the message. If the message is accepted, appropriate investigative action is taken. Please refer to the 'Investigation' section below. The whistleblower must receive an acknowledgement of receipt of the report within 7 days, and the investigation team must get back to the whistleblower with a response within 3 months of the date of receipt of the alert.

The investigation team may reject the alert under the following conditions (not cumulative):

- ✓ the behaviour reported does not constitute a case for launching an alert under these reporting guidelines;
- ✓ the message was not written in good faith, or is malicious;
- ✓ there is insufficient information to conduct an investigation;
- ✓ the content of the message has already been handled.

### **INVESTIGATION**

All messages are treated carefully and with strict respect for the rules of confidentiality described in these reporting guidelines.

- ✓ No one in the investigation team, and no one involved in an investigation, should seek to identify the person making a report.
- ✓ The investigation team may, if necessary, submit follow-up questions via the anonymous communication channel.
- ✓ The investigation of an alert will never be entrusted to a person likely to be involved in, or linked to, the issue raised.
- ✓ Internal or external experts may be included in the investigation with the whistleblower's consent.

If a person is the subject of an investigation, that person will be notified in a timely manner, unless doing so would seriously undermine the investigation or the delay in notifying is otherwise justified.

## **Protection of privacy**

### **WHISTLEBLOWER PROTECTION**

A person who reports a genuine suspicion or concern must not risk losing their job or suffer any form of reprisal or personal or professional disadvantage whatsoever. Whistleblowers should not be sanctioned for raising an alert or suspicion, as long as they are acting in good faith.

Subject to respect for the right to personal data protection of persons reported, identified whistleblowers must be informed of the outcome of the investigation.

In the case of reports of suspected criminal offences, the person making the report is informed, subject to their consent, that their identity may be disclosed to the relevant judicial authorities.

### **PROCESSING OF PERSONAL DATA**

This whistleblowing service may collect personal data about the person named in a report, the person who sends the report (if it is not sent anonymously) and any third parties involved, in order to

investigate the facts relating to reported breaches and misconduct covered by our code of conduct or internal rules. This processing may be based on a legal obligation or our legitimate interest in preventing reputational risks and promoting ethical business. The description and facts provided in the context of this processing are reserved solely for competent and authorised persons who treat this information as confidential. You may exercise your rights of access, rectification and objection, as well as limiting the processing of your personal data in accordance with local data protection legislation. These rights are subject to the necessary safeguards and security measures to prevent the destruction of evidence or other impediments to the processing and investigation of the case. For any other questions or complaints, please send your request to our data protection compliance team at [dataprotection@bakertilly.lu](mailto:dataprotection@bakertilly.lu).

#### **DELETION OF PERSONAL DATA**

Personal data contained in reports and investigation documentation are deleted once the investigation has been completed, except where their retention is required under the applicable legislation. The platform allows files to be permanently deleted 30 days after the end of the investigation. Investigation attachments and archived reports must be anonymised in accordance with the GDPR; archived messages must exclude personal data that directly or indirectly identifies individuals.

#### **DATA CONTROLLER :**

Baker Tilly is the controller of the personal data processed as part of the whistleblowing service.

#### **DATA PROCESSORS :**

WhistleBox BV (3290 Diest, Statiestraat 41, registered with the Crossroads Bank for Enterprises under number 0754.832.521) and Grant Thornton Advisory act as processors for data processing activities carried out on behalf of and under the instructions of Baker Tilly (the data controller). Neither WhistleBox nor Grant Thornton Advisory are able to decrypt or read messages transmitted anonymously.