

PRIVACY NOTICE

Whistleblowing Point of Contact

At Eurofins Group (“Eurofins” or “we”), ethical conduct, integrity and compliance with applicable laws form a fundamental part of our culture and business operations. Our clients, suppliers, employees and other stakeholders must be able to rely on absolute integrity from our part, and we must be able to rely on the integrity of our business partners.

Therefore, we encourage any individual who has genuine concerns about any form of malpractice or wrongdoing in any Eurofins company to raise those concerns with us, at the earliest stage possible, to maximise the opportunity for a thorough investigation and appropriate remediation. This Whistleblowing Point of Contact was established to provide you with a reliable and transparent channel to communicate your concerns to us. We also invite you to consult the Eurofins Group Whistleblowing Guidelines for various details of our Group’s whistleblowing policy.

When raising a concern be assured that we respect you, and we are committed to honouring and protecting your privacy. We treat personal data in accordance with applicable data protection laws (specifically the EU General Data Protection Regulation – “GDPR”), and the purpose of this notice is to make you aware of what personal data we collect and how we process them for the purposes of verifying concerns reported via the Whistleblowing Point of Contact and investigating suspected compliance or legal violations.

Who is your personal data controller?

The controller of your personal data is **Eurofins International Support Services LUX sàrl** with offices at: 23 Val Fleuri, L-1526 Luxembourg, Grand-Duchy of Luxembourg.

If you have any questions regarding this notice or if you want to lodge a request in relation to your personal information, **please contact us via the following contact point:**

dp-compliance@sc.eurofinseu.com

What personal data do we collect and how will it be processed?

We need to process sufficient information from you to be able to properly investigate your concerns, including any evidence that you may share to support them. We will collect and process the following personal data:

- e-mail address or other contact details used to submit the report;
- your name and surname as well as your other contact details if you decided to provide them to us. Please note that you can choose to **contact us anonymously**, but we are more likely to be able to protect you, investigate your concerns¹ and keep you informed about our progress if you identify yourself;
- other information you have given to us, including the identity, position, location and contact details of individuals subject of your concerns and any potential witnesses.

If you identify yourself (which means that you do not raise your concerns anonymously), we will maintain the confidentiality of your identity and any information from which your identity could be directly or indirectly inferred, except where disclosure is required by law or is necessary and proportionate in the context of investigations, legal proceedings, or regulatory requirements.

¹ In certain cases, and some jurisdictions, anonymous reporting is not permitted, and we will not be able to take appropriate action if you do not disclose to us your identity.

Personal data relating to reporters, individuals concerned by a report, witnesses and any other persons identified during an investigation may be processed where necessary for the handling of a whistleblowing report.

Reports may also contain special categories of personal data within the meaning of Article 9 GDPR and information relating to criminal offences or alleged offences. Such data will only be processed where necessary and permitted under applicable law, including for the establishment, exercise or defence of legal claims, compliance investigations, and fulfilment of legal obligations.

What are the purposes and legal grounds for processing personal data?

Personal data will be processed solely for the purposes of receiving, recording, assessing and appropriately segregating reports submitted through the Whistleblowing Point of Contact, investigating allegations raised in such reports, implementing any necessary remedial actions, and preparing records, reports and other documentation relating to the assessment and outcome of relevant investigations.

The processing of personal data is carried out on the following legal bases:

- **Compliance with a legal obligation** pursuant to Article 6(1)(c) GDPR, where required by applicable whistleblowing legislation, including national laws implementing Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law;
- **Legitimate interests pursued by Eurofins** pursuant to Article 6(1)(f) GDPR, namely to promote and maintain a culture of ethics, integrity and compliance; to ensure adherence to the Eurofins Group Code of Ethics, internal policies and procedures, and applicable laws and regulations (including, where relevant, employment, anti-corruption, anti-fraud, anti-money laundering, sanctions, modern slavery and similar regulatory requirements); and to enable the confidential reporting, assessment, investigation and remediation of actual or suspected misconduct, wrongdoing or legal and compliance violations throughout the Eurofins Group;
- **Employment and social security law** pursuant to Article 9(2)(b) GDPR, when processing the special categories of personal data is strictly necessary to perform obligations or exercise specific rights in the field of employment law (e.g., investigating workplace discrimination, harassment, or occupational safety breaches);
- **Establishment, exercise or defence of legal claims**, including the protection and enforcement of Eurofins' legal rights and interests in administrative, regulatory, disciplinary or judicial proceedings, pursuant to Article 6(1)(f) GDPR and, where applicable, Article 9(2)(f) GDPR in relation to special categories of personal data.
- **Substantial public interest** pursuant to Article 9(2)(g) GDPR, when the report covers areas of significant public interest explicitly regulated by the applicable legislation (e.g., anti-money laundering, public health, or financial market integrity).

How are we securing personal data?

We have implemented industry standard security measures to keep personal data **secured and confidential**, including but not limited to:

- by way of limiting access to personal data to authorised members of the Eurofins Group Compliance and Legal functions, including personnel located within Eurofins entities that provide compliance support services to the Group. Such personnel act solely under appropriate confidentiality obligations, documented instructions, and **strictly on a need-to-know basis**;
- by implementing physical, electronic, administrative, technical and procedural safeguards (such as data minimisation, data partitioning, anonymisation, encryption) that comply with applicable laws and regulations to protect personal data from unauthorised or inappropriate access, alteration, disclosure and destruction.

For how long will we keep personal data?

Personal data will be retained only for as long as necessary to investigate the report, implement any resulting actions, comply with legal obligations, and establish, exercise or defend legal claims.

With whom can we share personal data?

Personal data may be shared, strictly on a need-to-know basis, with Eurofins Legal Entities (<https://location.eurofins.com/en/>) for the purposes of taking relevant remedial actions following the investigation and / or our external legal advisors, forensic experts, auditors or other professional advisers, acting either as independent controllers or processors, depending on the nature of their engagement.

We may also send personal data to regulatory or law enforcement authorities if we believe in good faith that we are required by law to disclose them, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings.

Where relevant, personal data will be shared only on the basis of relevant agreements that include appropriate safeguards for protecting personal data in compliance with respective data protection regulations.

Where personal data is to be shared with recipients outside European Union / European Economic Area, located in countries for which there is no adequacy decision of the European Commission, the relevant transfer mechanism shall be adopted, such as Binding Corporate Rules ("BCRs"), the Standard Contractual Clauses adopted by the European Commission ("SCCs"), or another lawful transfer mechanism recognised under applicable data protection laws.

What rights do you have in relation to processing of your personal data?

In relation to processing of your personal data, you have the rights to: access data, rectify data, restrict the processing of data, require erasure of data as well as object to the processing of data (where justified and our legitimate interest in processing such data is not overriding data subjects' interests or the fundamental rights and freedoms).

Depending on the circumstances and applicable law, the exercise of certain rights may be restricted where necessary and proportionate to protect the confidentiality of whistleblowers, preserve the integrity of investigations, safeguard the rights of others, or comply with legal obligations.

At all times, you also have the right to lodge a complaint to the national data protection authority in Luxembourg:

Commission Nationale pour la Protection des Données (CNPd)

Location: 15, Boulevard du Jazz, L-4370 Belvaux, Grand-Duchy of Luxembourg

Tel.: +352 26 10 60-1

<https://cnpd.public.lu/en.html>

By submitting a report through this Whistleblowing Point of Contact, you acknowledge that your personal data will be processed in accordance with this Privacy Notice and applicable data protection laws.