



The Eurofins Group Privacy Policy

We take steps to ensure that personal information is collected, used and shared lawfully, in accordance with applicable data protection and privacy laws, and that the confidentiality and integrity of personal information is upheld.

Message from Eurofins CEO, Dr. Gilles Martin



THE EUROFINS STANCE TOWARDS DATA PROTECTION AND PRIVACY

The position of the Eurofins Group¹ towards data protection and privacy is clearly described in the Eurofins Group Code of Ethics:

“Eurofins is committed to treating information with respect and protecting personal data from unauthorised disclosure.”

The Eurofins Group respects the privacy of its employees, customers and other individuals whose personal information it processes in the course of its business activities. We take steps to ensure that personal information is collected, used and shared lawfully, in accordance with applicable data protection and privacy laws (“**DPP Laws**”), and that the confidentiality and integrity of personal information is upheld.

PURPOSE OF THIS POLICY

This Policy explains common obligations imposed by DPP Laws globally, and sets out common standards adopted by the Eurofins Group to manage its overall adherence to DPP Laws. The Eurofins Group has its central place of administration in Luxembourg, where the applicable data protection law is the General Data Protection Regulation. However, this Policy is not specific to any jurisdiction or legal regime, and it does not prescribe operational processes necessary to maintain ongoing compliance with locally applicable laws. Responsibility for this task is with each Eurofins Company, to be managed in the context of its day-to-day activities and its particular exposure to personal information and the local laws governing the use of that information.

HOW THIS POLICY WORKS

This Policy applies across all Eurofins Companies and to all of their leaders, directors and employees (referred to in this Policy as “**Eurofins Members**”).² Each Eurofins Company will ensure that any third party (individual or organisation), for whose conduct that Eurofins Company may be responsible, complies with standards at least as rigorous as this Policy. This applies to any person acting for, or on behalf of, any Eurofins Company (referred to in this Policy as “**Associate**”). Companies and joint ventures in which the Eurofins Companies do not have a controlling interest should be provided with a copy of and requested to apply this Policy.

The Policy is meant to set a general standard applicable throughout the Eurofins Companies. It does not override requirements of local laws: whenever a local law specifies stricter requirements than this Policy, the local law shall always prevail. As compliance matters are governed by local laws, this Policy has to be read as providing recommendations and guiding principles, not as a legally binding document committing any Eurofins Company. This Policy should be implemented in local policies, rules and processes by each Eurofins Company, in accordance with locally applicable laws.

This Policy should be read in conjunction with the [Eurofins Group Code of Ethics](#).

KEY TERMINOLOGY

DPP Laws are concerned with the protection of personal information, and with upholding the right of an individual to a private life. Personal information (also referred to as personal data) is generally understood to be any information (in most cases irrespective of form) which could be used to identify a natural person. This includes information such as names, dates of birth, contact details, and identification numbers, and may also include opinions about an individual, or statements about an individual’s behaviour or actions. It also encompasses categories of information which may be relevant to certain of Eurofins’ testing services, such as information about an individual’s physiology, their health conditions, information about their unique genetic characteristics, and physical or physiological biometric identifiers.

This Policy also refers to the “processing” of personal information, which is understood broadly as any activity performed with personal information. This can include (without limitation) collection, analysis, storage, modification, access to and disclosure of personal information.

¹ Eurofins or Eurofins Group or “we” means Eurofins Scientific SE and any entity directly or indirectly controlled by it, each individually referred to as a “Eurofins Company”.

² The terms leader, director, employee, Eurofins Member, Associate, Intermediary and any other terms designating persons or groups of persons as well as the terms “he” or “she” in this Policy are not meant to specify any gender and are to be read as being strictly non-discriminatory.



Certain categories of personal information are regarded by many DPP Laws as being particularly sensitive. These include categories such as health, genetics, biometrics, race and ethnic origin and religion, as well as government or national identifiers, personal financial information such as bank account details, and account passwords.

PROCESSING OF PERSONAL INFORMATION BY EUROFINS

In providing its testing services to clients, companies belonging to the Eurofins Group process personal information which comprises, or is attached to, the samples or materials which it tests. This can include health, genetic and biometric data, and patient, clinical trial or research study participant identifiers. Test data may be pseudonymised or otherwise de-identified before it is processed by Eurofins Companies.

Outside of test data, the Eurofins Group processes personal information about its clients and suppliers for client and supplier relationship management, marketing and finance purposes, as well as for general business administration.

Finally, each Eurofins Company also processes personal information about its own employees, workers and job applicants, as well as its suppliers and vendors of goods and services, visitors to Eurofins Companies' premises, Eurofins Companies' websites users and those who submit general inquiries.

KEY PRINCIPLES

The following principles are reflected in many DPP Laws, and should be applied as a minimum standard across the Eurofins Group to each Eurofins Company's processing of personal information:

- personal information will be processed in a fair, lawful and transparent manner;
- personal information will be obtained for specified purposes and will not be processed in any manner incompatible with those purposes, except where permitted by law;
- personal information will be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed;
- personal information will be accurate and, where necessary, kept up to date;
- personal information will not be kept for longer than is necessary;
- appropriate measures will be taken to safeguard personal information against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Each Eurofins Company will ensure that each Eurofins Member and Associate is aware of these principles, and understands his or her obligation to apply them to their work.

GOVERNANCE

It is essential that strong governance controls exist within the Eurofins Group, at both a local and group-wide level, to ensure that compliance is monitored and supported on an ongoing basis. Data protection and privacy is recognised as a key risk issue by the senior management of the Eurofins Group, and each Eurofins Company is expected to dedicate appropriate resources to data protection compliance.

Before launching a new project or way of working (or making changes to an existing project or way of working) which processes significant volumes of personal information, or which involves processing personal information in ways that are novel or high risk, each Eurofins Company will consider the associated privacy risks and take steps to mitigate or eliminate those risks. In so doing, Eurofins Companies will apply the principles of "privacy by design" in order to reduce inefficiency and prevent intervention becoming necessary at a later date. Where required by applicable laws, a Eurofins Company will complete a data protection impact assessment, or other similar formal risk assessment.

Many DPP Laws require the appointment of a data protection officer or another responsible individual. When required, the Eurofins Company concerned will be responsible for ensuring an appropriate appointment is in place, and that the individual in question receives necessary training and support.



DATA SECURITY AND INCIDENT REPORTING

The Eurofins Group recognises the importance of implementing appropriate technical and organisational measures to safeguard the security of personal information. To this end, the Eurofins Group has implemented a group-wide Information Security Policy, which contains minimum standards designed to protect information assets, including personal information. Measures include (without limitation, and in each case where appropriate in the context):

- encryption, data masking and data aggregation;
- technical controls to detect and prevent unauthorised access to Eurofins systems;
- the restriction of access to personal information on a “need-to-know” basis and the use of role-based access control;
- vulnerability and penetration testing;
- the regular testing of security measures to ensure their ongoing fitness for purpose;
- business resilience and disaster recovery processes designed to ensure the prompt restoration of availability to personal information; and
- set of Eurofins security policies, which define minimum acceptable controls, and which are imposed on Eurofins Companies.

The Eurofins Group also recognises the importance of each Eurofins Member and Associate assuming personal responsibility in this area. Eurofins Companies will take steps to ensure that Eurofins Members and Associates are aware of their role in safeguarding information security.

Where a Eurofins Company detects an incident in which the security of personal information has been compromised, it will take steps to investigate and remediate that incident, and will comply with any notification obligations (either to a Eurofins client or to a regulator) under applicable laws.

SHARING PERSONAL INFORMATION

Eurofins Companies will only share personal information with third parties where there is a business need and it is lawful to do so, or in response to a legal requirement, or a lawful request from a regulator, other government body or court. Before sharing personal information, each Eurofins Company will establish the purpose for which the personal information is required, and (where the request is otherwise lawful) will share only the minimum personal information required for that purpose.

Where a Eurofins Company engages a third party to process personal information on its behalf (including, without limitation, sub-contractors, IT service providers, and suppliers of business process outsourcing solutions), it will:

- abide by the requirements set forth in the Eurofins policies ensuring lawful processing of personal information;
- enter into a written agreement with the third party, which imposes appropriate terms in relation to the confidentiality, security and processing of personal information, including any terms required by applicable laws; and
- respond promptly to any concerns regarding the third party’s ongoing ability to comply with DPP Laws.

INTERNATIONAL TRANSFERS

Many DPP Laws place absolute or conditional restrictions on transferring personal information across international borders. In this context, the term “transfer” can be understood widely, and may refer to mere remote access to personal information from a foreign jurisdiction. Certain work undertaken by the Eurofins Group is “cross-border” in nature, and transfers may occur both between a Eurofins Company and a client, as well as between two Eurofins Companies.

All Eurofins Companies shall ensure that personal information is shared between them internationally observing the DPP Laws provisions relevant for such international transfers as well as in accordance with mutually agreed obligations concerning the protection of the information which is shared.

Further, each Eurofins Company is responsible for ensuring that transfers of personal information which it initiates with third parties (for example, with clients or suppliers) are lawful. This may entail (without limitation):

- notifications to and/or approvals obtained from local regulators;
- adherence to specific contractual obligations;
- certification under appropriate schemes; and
- the maintenance of locally hosted databases / copies of transferred data.



“CONTROLLER” AND “PROCESSOR” CATEGORISATIONS

Some DPP Laws distinguish an organisation that decides ‘how’ and ‘why’ personal information is processed (referred to in this Policy as the “controller”) from an organisation which processes personal information solely on behalf of, and subject to the instructions of, a controller (referred to in this Policy as the “processor”). A processor may also have responsibilities under applicable laws, but these will be different in scope from the controller’s. Eurofins Companies may be treated not only as the controllers but also as the processors for certain activities and shall follow the respective DPP Laws provisions depending on their specific roles in the given activities.

TRANSPARENCY

DPP Laws may require Eurofins Companies to explain to individuals how and why their personal information is used, and to give them information about their rights and how these can be exercised. Transparency obligations typically apply where a Eurofins Company is acting as a controller, or in an equivalent role.

Where required by DPP Laws, privacy notices will be provided to Eurofins Members and to other natural persons whose personal information is processed by a Eurofins Company. These notices will be clear and accurate, and will contain all information which is required by applicable law, including (where required) information about the rights available to the natural person, and how those rights may be exercised.

All Eurofins Group websites will contain privacy notices and disclaimers appropriate to the scope and nature of the website, and the jurisdiction(s) at which the website is targeted.

INDIVIDUAL RIGHTS

Natural persons may have rights under DPP Laws, which can be exercised in order to (without limitation):

- find out how and why their personal information is being processed;
- access a copy of their personal information;
- amend or delete their personal information;
- restrict or prevent the processing of their personal information, or its disclosure to a third party;
- object to a specific use of their personal information; or
- have their personal information transported to another organisation.

The Eurofins Group is committed to cooperating with individuals regarding the protection of their privacy, and to helping individuals exercise their rights under DPP Laws, and to responding to their requests diligently and completely (or where a Eurofins Company is processing personal information on behalf of a client, assisting that client to do so). This includes implementing appropriate processes for responding to requests within applicable timescales, including, where appropriate and reasonably possible, technical solutions necessary to retrieve and edit personal information.

ENFORCEMENT AND SANCTIONS

If a Eurofins Company is found to be in breach of applicable DPP Laws, it could face fines and other enforcement actions (such as order prohibiting data usage) taken against it by regulators. Prior to enforcement action, Eurofins Companies may be subject to regulatory audits and inspections which may, *in extremis*, be conducted on a limited or no notice basis.

Many DPP Laws also provide impacted individuals with private rights of action against Eurofins Companies in order to award compensation for breaches of DPP Laws. Compensation may be available even where no pecuniary losses have been incurred by the impacted individual, but where that individual is able to demonstrate that they have suffered distress.

REPORTING

Data protection and privacy compliance is a responsibility which applies to everyone within each Eurofins Company. If a Eurofins Member or an Associate has concerns about any actual or potential violation of this Policy, they should report those concerns at the earliest possible stage with their direct supervisor in a Eurofins Company, or the President



or Managing Director of the Eurofins Company concerned, or the relevant Eurofins Local Compliance Officer or legal department. If for any reason, you would prefer to report your concerns beyond the Eurofins Company concerned, you may contact or the Group's GDPR Compliance Counsel or the [Whistleblowing Point of Contact](#) (see below).

RISK ASSESSMENTS

The Presidents or Managing Directors and Local Compliance Officers of Eurofins Companies are required to review and assess the suitability of the operational policies and controls which they have in place to manage data protection compliance on at least an annual basis. As part of this review, each Eurofins Company should take steps to assess the extent to which those controls are being followed by Eurofins Members and Associates in practice. Finally, each Eurofins Company must also have processes in place (including, where appropriate, support from external subject matter experts) to ensure that it keeps up-to-date with developments in locally applicable DPP Laws, and reflects those changes within its operational policies and controls.

COMMUNICATION AND TRAINING

This Policy shall be communicated to each President or Managing Director of a Eurofins Company, who must confirm in writing that they have received, understood and will comply with this Policy and have or shall have implemented it into a binding local policy in compliance with, and as required by, local laws. This Policy is also available on Eurofins Group Intranet (DMS).

It is the obligation of each President or Managing Director to further communicate the content of this Policy to all Eurofins Members and Associates under their responsibility, and to ensure those reporting to them, or acting for or on behalf of the Eurofins Company they are in charge of, are made aware of and understand the Policy.

The Eurofins Group Service Centre will develop and implement a suitable training programme on data protection and privacy matters for all Eurofins Members. This will be the responsibility of the GDPR Compliance Counsel. Presidents and Managing Directors of Eurofins Companies are responsible, and will take such measures as may be necessary to ensure that all persons reporting to them follow this or a similar adequate local training as well as any additional required or appropriate local training in locally applicable data protection, privacy and information security standards including, as a minimum, the standards set out in this Policy.

GENERAL QUERIES

Individuals are encouraged to communicate any questions about this Policy and its application to their direct supervisors in Eurofins Companies or the relevant Eurofins Local Compliance Officers or legal departments. If you are unsure who to speak to, or if you would prefer to communicate questions beyond the Eurofins Company concerned, please contact the Compliance Helpline on the Company's intranet site (DMS).

WHISTLEBLOWING POINT OF CONTACT

Eurofins has a Whistleblowing Point of Contact that is readily accessible for all Eurofins Members and Associates via the Eurofins Group Intranet (DMS) and Eurofins website, via the following link: <https://www.eurofins.com/about-us/corporate-sustainability/governance/whistleblowing/> (the "Whistleblowing Contact"). The Whistleblowing Contact is also available to any third party.

The Whistleblowing Contact is intended to encourage and enable Eurofins Members, Associates and third parties to confidentially raise concerns in respect of non-compliance with this Policy (or with the Eurofins Group Code of Ethics or any other Eurofins Company policy or any applicable laws) without fear of retaliation by Eurofins, so that the Eurofins Companies can take prompt action to address and correct inappropriate conduct or actions.

On behalf of the Eurofins Group Operating Council

Dr. Gilles Martin
Chief Executive Officer

