# Employee Privacy Notice

## Introduction

This Privacy Notice explains how Eurofins Forensic Services Limited (“we”, “us”, “our”) collect, use, and protect personal data relating to employees, workers, agency staff, contractors, and applicants.

As a forensic services provider, we process personal data in a highly regulated environment that requires strict security, integrity, and audit controls. We are committed to handling all personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Forensic Science Regulator’s Code of Practice, and all applicable accreditation standards.

This Notice describes what data we process, why we process it, how long we keep it, who we share it with, and your rights.

## Contact Details

The Data Protection Officer (DPO) oversees our compliance with data protection legislation and acts as the main contact point for privacy-related queries.

We are committed to protecting your personal data and take our responsibilities seriously. We handle your information with care to ensure proper processing, maintaining your trust and confidence. If you have any questions or concerns about how we manage your personal data, our DPO is available to assist you.

Email: dpo@forensicsuk.eurofins.com

Address: Data Protection Officer, Eurofins Forensic Services, Sir Alec Jeffreys Building, Peel Avenue, Calder Park, Wakefield, WF2 7UA

## The UK GDPR Data Protection Principles

We adhere to the seven key principles set out in Article 5 of the UK GDPR.

1. Lawfulness, Fairness and Transparency
   We process personal data lawfully, fairly, and in a transparent manner. Employees are informed about how their data is used through this Privacy Notice and other relevant policies/notices.

2. Purpose Limitation

We collect personal data for specific, explicit, and legitimate purposes and do not use it for purposes that are incompatible with those original purposes.

3. Data Minimisation
   We only collect the personal data that is necessary for the purposes for which it is processed.

4. Accuracy
   We take reasonable steps to ensure personal data is accurate and kept up to date. Employees are encouraged to notify HR or the DPO of any changes to their information.

5. Storage Limitation
   We keep personal data for no longer than is necessary for the purposes for which it was collected. Retention is governed by our internal retention schedule and applicable regulatory requirements.

6. Integrity and Confidentiality (Security)
   We handle and store personal data securely using appropriate technical and organisational measures to protect against unauthorised access, loss, destruction, or damage.

7. Accountability
   We are responsible for, and can demonstrate compliance with, all of the data protection principles. This includes maintaining documentation, providing training, conducting DPIAs where needed, and ensuring robust oversight.

**What Personal Data We Process**

We collect and process the following categories of data:

a. Identification and Contact Information
- Name, address, personal email, personal telephone number
- Date of birth, gender
- Emergency contact details, next of kin, dependants
- Proof of identity and right-to-work information

b. Employment and HR Records
- Employment contracts, CVs, qualifications, training records
- Performance reviews, objectives, notes of supervision meetings
- Attendance, rota, timekeeping, annual leave, sickness absence
- Grievance and disciplinary records (where applicable)

c. Financial and Payroll Information
- Bank details
- Salary, tax, National Insurance, pension and benefits information

d. Special Category Data

We may process special category data, including:

- Health data (e.g. occupational health assessments, fitness for work)
- Equality and diversity data (e.g. ethnicity, disability; if you choose to provide it)
- Trade union membership
- Genetic and biometric data – DNA profiles

e. Criminal Records Data

Due to the sensitive nature of our work, we process:

- Security vetting results
- Criminal conviction or barring information where required

f. Security, Monitoring and Access Control Data

To maintain forensic integrity, chain-of-custody controls, and site security, we collect:

- CCTV footage
- Door access logs, security pass usage
- IT system logs, device usage, email and network monitoring
- Audit trail data relating to laboratory systems and evidential processes

g. Recruitment Information

- Application forms, interview notes
- Pre-employment screening reports
- Professional reference information

The types of personal data we process will vary depending on the purpose. We aim to process the minimum amount of personal data necessary for the relevant purpose. You should not assume that we hold personal data in all of the categories identified for every person whose personal data we process.

Please note that the categories listed above may not be exhaustive. In certain cases, we may process other types of personal data where necessary to fulfil our contractual or legal obligations.

## How We Collect Personal Data

We collect information:

- Directly from you
- Automatically through access control, CCTV, or IT monitoring
- From third parties, such as referees, recruitment agencies, DBS services, and occupational health providers
- From internal systems (HR, laboratory systems, security systems)

## Purposes of Processing

We ensure that all personal data is processed lawfully, fairly, and transparently, in accordance with applicable data protection legislation.

We process your personal data for the following purposes:

Employment and HR Management

- Recruitment, onboarding and vetting, including providing references for current or former employees
- Pay, pensions, and benefits
- Managing and recording performance, conduct, and development
- Managing absences, sickness, leave, and return-to-work assessments

Legal and Regulatory Compliance

- Meeting obligations under employment, tax, and health & safety law
- Maintaining accreditation standards (e.g. FSR Codes, ISO/IEC 17025, ISO/IEC 27001)
  - This includes maintaining a Staff Elimination Database (SED)
- Responding to audits, inspections, and regulatory enquiries

Security, Integrity and Operational Control

- Securing our premises and laboratory environments
- Maintaining secure access to evidential materials
- Monitoring compliance with IT and data security policies
- Detecting, investigating, and preventing misconduct or security breaches

Business Management

- Workforce planning, reporting, and forecasting
- Ensuring continuity of operations
- Allowing for the management of complaints or legal claims
- Submitted as part of a bid or tender for customer contracts

**Lawful Bases for Processing**

We process personal data for the following purposes, relying on the legal bases set out under the UK General Data Protection Regulation (UK GDPR):

For standard personal data

- Contract – necessary to enter into or fulfil your employment contract
- Legal obligation – e.g. tax reporting, H&S requirements
- Legitimate interests – e.g. lab security, access control, performance management
- Consent – rarely used; only for optional activities (e.g. wellbeing initiatives, donor samples)

For special category data

- Explicit consent
- Employment, social security, and social protection law
- Occupational health obligations
- Equality monitoring
- Establishment, exercise, or defence of legal claims
- Substantial public interest (e.g. safeguarding, preventing fraud)

For criminal offence data
Processed under Schedule 1 DPA 2018 conditions, where vetting is necessary for roles involving secure environments and access to evidential material.

Where we rely on legitimate interests, we ensure that our interests are not overridden by the rights and freedoms of individuals.

**Automated Decision-Making**

We do not make employment decisions based solely on automated processing.

**Who We Share Personal Data With**

We only share personal data where it is necessary, lawful, and proportionate to do so.

We may share personal data with:

- Payroll, pension, and benefits providers
- Recruitment agencies and vetting services
- Government bodies (HMRC, Home Office, ICO where appropriate)
- Professional and accrediting bodies
- Occupational health and wellbeing providers
- IT service providers and system hosts
- External auditors
- Legal advisors and insurers
- Customers and clients
- Other Eurofins entities

We only share the minimum data necessary and ensure appropriate safeguards are in place.

**International Transfers**

We do not routinely transfer personal data outside the UK. If such transfers are necessary, we ensure appropriate safeguards are in place (e.g. adequacy decisions, standard contractual clauses).

In most cases, personal data processed by Eurofins Forensic Services Limited is stored and handled within the UK. However, there may be limited circumstances where personal data is transferred to, or accessed from, countries outside the UK.

International transfers may happen when:

- We use secure cloud-based services or IT infrastructure hosted outside the UK
- We engage with approved third-party service providers or subcontractors based in other jurisdictions
- Data is accessed remotely by authorised personnel or partners located outside the UK for operational or support purposes
- We are required to share personal data with prospective and existing clients located outside of the UK as part of bid and tender processes, as well as for ongoing contractual work

You can request details of relevant safeguards at any time.

**Data Retention**

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, and in accordance with our contractual obligations, legal requirements, and industry standards. Examples include:

- HR employment file: 6 years after employment ends
- Payroll records: 7 years after employment ends
- Health and safety records: duration set by law

We maintain internal retention schedules and policies that govern how long different categories of personal data are held. These policies are regularly reviewed and updated to ensure compliance with UK legislation.

When personal data is no longer required, we ensure it is securely deleted or destroyed in accordance with our data disposal procedures and industry standards.

**Security Measures**

We implement a range of technical, organisational, and procedural measures to protect personal data from unauthorised access, loss, misuse, alteration, or destruction. We comply with our legal obligations regarding security, and relevant controls of the ISO27001 Information Security Standard.

Technical Measures

- Password Management: Access to systems and applications is protected by complex password policies
- Access Controls: Role-based access controls ensure that only authorised personnel can access specific categories of personal data
- Secure Networks: Our systems operate within secure network environments protected by firewalls, intrusion detection systems, and endpoint protection

Organisational Measures

- Staff Training: All employees receive regular training on data protection, information security, and confidentiality obligations
- Policies and Procedures: We maintain comprehensive internal policies covering data handling, incident response, and secure disposal
- Supplier Assurance: Third-party service providers are subject to rigorous due diligence and contractual obligations to ensure data protection compliance

Physical Security

- Secure Facilities: Forensic laboratories and data centres are protected by physical access controls, CCTV monitoring, and visitor management systems
- Controlled Storage: Physical evidence and records are stored in secure, access-controlled environments

Incident Management

- We have a formal incident response plan in place to detect, report, and respond to data breaches or security incidents promptly
- Any incidents involving personal data are assessed and, where required, reported to the relevant data controller and the Information Commissioner's Office (ICO) in accordance with legal obligations

**Your Rights**

Under the law, including the Data Protection Act 2018, UK GDPR, and the Data Use and Access Act 2025 (DUAA), you have a number of rights in relation to the personal data we process about you. You do not have to pay to exercise your rights (except where a request is clearly unfounded or excessive, in which case we may charge a reasonable fee if we agree to fulfil it).

- Right of access
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to portability
- Right to object to processing
- Right to withdraw consent (if we rely on consent)
- Right to complain (New under DUAA 2025) – If you believe your personal data has been processed unlawfully or unfairly you have the right to submit a complaint directly to us. We encourage you to include:
    - Your full name and contact details
    - A clear description of your concern
    - Any supporting documentation, if relevant

Please refer to EFS-DIV-4863 *Data Protection Complaints Policy* for full details of our complaints procedure, or request a copy via the email address below if preferred.

If you wish to exercise any of your rights, please contact:

Data Protection Officer

Email: dpo@forensicsuk.eurofins.com

If you are dissatisfied with how your personal data has been handled, or with the response to a complaint, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Website: www.ico.org.uk
Phone: 0303 123 1113
Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

**Notice Updates**

We keep this privacy notice under regular review and update it if any of the information in it changes. The latest version will always be available on the Quality Management System or upon request.

Last reviewed and updated on 18/05/2026.