Data Privacy Notice

Introduction

Eurofins Forensic Services (EFS) Limited ("we", "us", "our") is committed to protecting and respecting personal data. This Privacy Notice explains how we collect, use, and protect personal data when carrying out our activities.

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 is intended for members of the public and other individuals whose personal data may be processed by us.

We also maintain separate, more detailed privacy notices for specific groups, including:

- Employees (Document Ref: EFS-DIV-2317 *Employee Privacy Notice*)
- Job applicants (Document Ref: EFS-DIV-2316 *Applicant Privacy Notice*)

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. Individuals 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.

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.

Our Role in Processing Personal Data

We process personal data in two capacities:

- As a data controller – where we determine how and why personal data is used
- As a data processor – where we process personal data on behalf of our clients/customers (the “controller”), in accordance with their instructions

Where we act as a processor, the controller is primarily responsible for determining how your personal data is used and for responding to your data protection rights.

If you contact us regarding such processing, we may:

- Redirect you to the relevant controller

- Assist the controller in responding to your request

What Personal Data We Process

We may process the following categories of personal data:

- Identification data (e.g. name, date of birth, gender, addresses, reference numbers)
- Special category data (e.g. genetic and biometric data such as DNA profiles)
- Case or service-related data (as provided by our clients/customers)
- Contact details (e.g. email address, telephone number)
- Correspondence and enquiry data

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.

Whose Personal Data We Process

We may process personal data relating to a range of individuals, including:

- Victims of crime
- Individuals who have been convicted of an offence
- Individuals suspected of committing an offence
- Complainants, correspondents, and enquirers
- Advisors, consultants, and other professional experts
- Suppliers and service providers
- Current and former employees, workers, agents, and volunteers

We may also process personal data relating to representatives of these individuals, including:

- Parents and guardians
- Family members or next of kin
- Individuals holding legal authority (e.g. power of attorney)

How We Collect Personal Data

We obtain personal data from:

- Our clients/customers (where we act as a processor)
- Individuals directly (e.g. enquiries, complaints)
- Third parties where appropriate and lawful

Purposes of Processing

We process personal data for the following purposes:

- Providing services on behalf of our clients/customers
- Managing enquiries and communications
- Handling complaints
- Ensuring quality assurance and service delivery
- Maintaining the security of our systems
- Complying with legal and regulatory obligations

Lawful Basis for Processing

Where we act as a data processor, we process personal data:

- On behalf of, and under the instructions of, our clients/customers
- In accordance with contractual and legal obligations

Where we act as a data controller, we rely on lawful bases such as:

- Legal obligations
- Legitimate interests (e.g. service improvement, complaint handling)
- Consent (where applicable)

Automated Decision-Making

We do not carry out automated decision-making that produces legal or similarly significant effects on individuals, unless explicitly stated.

Who We Share Personal Data With

We may disclose personal data to a range of recipients, including those located outside the United Kingdom and the European Economic Area (EEA), where necessary. This may include parties from whom the personal data was originally obtained.

EFS will only share personal data with third parties where this is necessary to fulfil contractual or legal obligations, or where otherwise permitted by law.

Recipients may include:

- Law enforcement agencies
- Local authorities, and national and local government departments and agencies (including, but not limited to, the Home Office, HM Revenue and Customs, the Serious Fraud Office, the Child Maintenance Service, and the National Fraud Initiative)
- Legal representatives, prosecuting authorities, courts, prisons, and other criminal justice partners
- Third parties acting on our behalf (e.g. service providers and sub-processors)
- Ombudsmen, auditors, and regulatory authorities
- Other bodies or individuals where disclosure is required or permitted by law, including under legislation or court order

Where personal data is transferred internationally, appropriate safeguards will be implemented in accordance with applicable data protection laws.

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 applicable industry standards.

Where we act as a data processor, retention periods are determined by our clients/customers. For example, relevant frameworks such as the Management of Police Information (MoPI) guidelines may apply.

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

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

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 data protection 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, unless your request is clearly unfounded or excessive. In such cases, we may charge a reasonable fee or refuse to act on the request where permitted by law.

You have the following rights:

- Right of access – You have the right to request a copy of the personal data we hold about you and information about how it is used.
- Right to rectification – You have the right to request that we correct inaccurate or incomplete personal data.
- Right to erasure (where applicable) – You may request that we delete your personal data where there is no lawful reason for us to continue processing it. This right does not apply in all circumstances.
- Right to restrict processing – You have the right to request that we limit how we use your personal data, for example while a concern about its accuracy or use is being investigated.
- Right to data portability – Where applicable, you have the right to receive your personal data in a structured, commonly used format and to request that it is transferred to another organisation.
- Right to object to processing – You have the right to object to the processing of your personal data in certain circumstances, particularly where processing is based on legitimate interests.
- Right to withdraw consent (where applicable) – Where we rely on your consent to process personal data, you have the right to withdraw that consent at any time.
- Right to complain – If you believe your personal data has been processed unlawfully or unfairly, you have the right to submit a complaint directly to us.

When submitting a complaint, we encourage you to include:

- Your full name and contact details
- A clear description of your concern
- Any supporting documentation, where relevant

Please refer to EFS-DIV-4863 *Data Protection Complaints Policy* for full details of our complaints procedure. A copy can also be requested via the contact details below.

Where we process personal data on behalf of a client/customer (as a data processor), you will need to exercise your rights directly with the relevant data controller. We will assist where required.

How to Contact Us

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

Data Protection Officer
Email: dpo@forensicsuk.eurofins.com

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

Right to Escalate

If you are not satisfied with our response, you may escalate your complaint to 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.

Last reviewed and updated on 19/05/2026.