



Experian Confidential Helpline – Privacy Notice

1. Introduction and Purpose

Experian provides access to a Confidential Helpline operated by Navex Global. This Privacy Notice explains how Experian processes personal data in connection with reports and concerns raised, including those submitted via the Confidential Helpline. It applies to all personal data processed by Experian in this context, regardless of the method by which a report is made. This Privacy Notice should be read alongside, and is intended to supplement, Experian's existing privacy policies.

This Privacy Notice supplements Experian's Global Whistleblowing Policy and should be read together with it. In the event of any inconsistency, applicable national whistleblowing laws and the relevant country-specific provisions prevail.

2. Who Can Use the Confidential Helpline

The Confidential Helpline is available to individuals who acquire information on actual or suspected wrongdoing in a work-related context, including but not limited to employees and former employees; contractors, consultants, agency staff, and interns; shareholders; members of administrative, management, or supervisory bodies; and individuals whose employment relationship has not yet begun.

3. How we process your personal data

Experian processes personal data in accordance with the principles set out in applicable data protection laws, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.



Experian processes the following categories of personal data in connection with concerns raised through its internal reporting channels, including the Confidential Helpline operated by Navex Global:

3.1. Categories of Individuals

Individuals who raise or disclose information relating to an actual or suspected wrongdoing (a concern), whether on an identified or anonymous basis.
Persons affected by a concern: individuals who are named or otherwise identifiable in a concern as being involved in or affected by the alleged wrongdoing, including persons whose conduct is subject to assessment during follow-up or investigation activities.
Witnesses and other relevant third parties: individuals identified as having relevant information in relation to a concern, including witnesses or other persons connected to the reported matter.
Other individuals named in a concern: employees, contractors, shareholders, board members, or external parties whose personal data is included in a concern or related documentation.
Authorised case handlers and investigators: employees or other authorised persons within Global Internal Audit (GIA), Compliance, Legal, Human Resources, or other designated functions who are competent to receive, assess, investigate, or follow up on concerns.

3.2. Categories of Personal Data

Depending on the nature of the concern, Experian may process the following categories of personal data:

Data Category	Description
Identification data	Personal data such as name or username.
Contact details	Information such as email address, telephone number, or other voluntarily provided contact information.
Employment or professional information	Details such as job title, department, reporting line, role, or relationship to Experian.
Concern and case-related information	Information including descriptions of allegations, dates, locations, individuals involved, and narratives.
Communications and supporting materials	Materials such as messages, attachments, transcripts, or minutes of oral reports.
Investigation and follow-up information	Data including case notes, findings, decisions, and actions.
Record-keeping or system data	Information such as timestamps, system-generated case references, audit trails, and activity logs.

4. Purposes of Processing

Experian may process personal data in order to:

- **Receive and acknowledge concerns raised**
Personal data is used to receive reports and ensure that concerns submitted through whistleblowing channels are properly logged and acknowledged.

- **Assess and investigate concerns**
Personal data is processed to review allegations, carry out appropriate investigations, and evaluate the validity and seriousness of the issues raised.
- **Determine outcomes and take remedial action**
Personal data supports decision-making on investigation outcomes, including identifying and implementing any necessary follow-up actions or corrective measures.
- **Communicate with whistleblowers**
Personal data is used to maintain communication with individuals who raise concerns, including providing updates where appropriate and requesting further information if needed.
- **Comply with legal and regulatory obligations**
Personal data is processed to meet applicable EU and national whistleblowing laws, as well as other legal and regulatory requirements.
- **Protect against retaliation**
Personal data is used to help prevent and address any form of retaliation against individuals who report concerns in good faith.
- **Safeguard rights and freedoms**
Personal data is processed to ensure the fair and balanced treatment of all individuals involved, protecting their rights and freedoms throughout the process.

5. Sources of Personal Data

Experian primarily obtains personal data directly from the Whistleblower, persons affected by a concern, witnesses, and internal investigations or supporting documentation generated during the handling of a case.

6. Access to Personal Data

Access to personal data relating to concerns is strictly restricted to individuals who have a demonstrable “need to know” for the purposes of receiving, assessing, investigating, and resolving such concerns. This includes Global



Internal Audit (“GIA”); designated representatives within Compliance, Legal, and Human Resources; duly authorised investigators and case handlers; and, where appropriate and in accordance with applicable law, external advisors, auditors, or competent public authorities. All such recipients are subject to appropriate confidentiality obligations and are required to process personal data in accordance with applicable data protection laws and internal policies.

6.1. Concerns raised via the Confidential Helpline

Where concerns are raised via the Confidential Helpline, the service is operated by Navex Global acting as a data processor on our behalf. Navex Global handles personal data solely in accordance with our documented instructions and for the purposes of intake, secure transmission, documentation, and preliminary case administration. Personal data submitted through the Confidential Helpline will be made available to Group Internal Audit (“GIA”) and, where strictly necessary, to other authorised recipients on a need-to-know basis to enable the appropriate assessment, investigation, and resolution of the concern.

6.2. Concerns raised via internal channels

Where concerns are raised through internal channels (including directly with Compliance, Legal, Human Resources, or GIA), the relevant personal data will be shared with GIA, which acts as the central function responsible for the oversight, coordination, and documentation of investigations. GIA will process such personal data for the purposes of case assessment, investigation, reporting, and compliance with legal and regulatory obligations.

In all cases, GIA will record and maintain personal data relating to concerns within the Confidential Helpline case management portal, for the purposes of ensuring consistent case handling, maintaining an auditable record of actions taken, and complying with applicable legal, regulatory, and internal governance requirements. Access to records within the portal is strictly controlled and limited to authorised personnel.

7. Confidentiality and Protection Measures

Experian applies strict confidentiality measures to all personal data processed in connection with concerns. The identity of the Whistleblower, persons affected by a concern, and any named third parties is disclosed only with the Whistleblower’s explicit consent or where required and proportionate under applicable law.



Whistleblowers will be informed in advance of any disclosure unless such notification would jeopardise investigations or proceedings.

8. Data Retention

Personal data relating to a concern will be retained only for as long as necessary and proportionate to fulfil the purposes of processing, in accordance with applicable whistleblowing and data protection laws.

Where an investigation is undertaken, personal data will be retained for the duration of the investigation and thereafter only for as long as necessary to conclude the matter and to establish, exercise, or defend legal claims, including applicable limitation periods. In addition, records of reports may be retained for a period that is necessary and proportionate to comply with legal and regulatory obligations.

Where an investigation is not undertaken (for example, when a concern is in fact a grievance that should be referred to the HR department instead), personal data and records of reports may be retained as necessary and proportionate for quality assurance and audit purposes.

9. Questions, requests and concerns

If you have any questions about how your personal data is processed, or you wish to request to exercise your data protection rights, you may contact Group Internal Audit (“GIA”) via the designated contact channel. GIA will deal with your request and, where relevant, engage with Legal and/or Compliance teams in the relevant country to ensure that your request is handled in accordance with applicable local data protection laws and requirements.

If you have a concern about data protection in the context of a whistleblowing report, or you believe that your personal data has not been handled in accordance with applicable laws or internal policies, we encourage you to raise this in the first instance by contacting your local Compliance team.

In many countries where we operate, you will also have the right to lodge a complaint with your relevant Data Protection Supervisory Authority if you are not satisfied with how we process your personal data, including in connection with whistleblowing matters



10. Updates to This Privacy Notice

This Privacy Notice may be updated periodically to reflect changes in applicable data protection laws, regulatory guidance, or Experian's whistleblowing arrangements. Where required, we will take appropriate steps to inform you of any material changes. The most current version of this Privacy Notice will always be made available, and we encourage you to review it regularly to stay informed about how your personal data is processed.



Annex – concerns raised by individuals located in the European Union (EU)

This annex explains how Experian complies with the General Data Protection Regulation (GDPR) and how data subjects can exercise their rights, in the context of concerns raised by individuals in the EU.

1. Data Processing roles and responsibilities

Where reports are submitted in connection with Experian entities in the EU (acting as Data Controllers), the relevant Experian EU entity shall act as a **Joint Controller** with Experian Limited (a United Kingdom entity).

The relevant Experian EU entities include:

- Experian GmbH etc
- *DACH team/Freshfields to confirm full list of entities party to the intra-group agreement*

In respect of the personal data contained in such reports, **the Experian EU entity** shall determine the data processing activities required, and have sole responsibility, for:

- the assessment, handling and investigation of concerns, and
- the identification of any remedial, disciplinary, or follow-up actions arising from such investigations

Experian Limited shall determine the data processing activities required for the administration, oversight, and governance of the Confidential Helpline operated by Navex Global, and Experian Limited's joint controllership shall not extend to operational decision-making regarding individual reports or investigations.

Navex Global shall act as a **Data Processor**, processing personal data solely on behalf of, and in accordance with the documented instructions of, the applicable Data Controller(s), as defined above.

This allocation of roles reflects the contractual framework between Experian Limited and Navex Global and is intended to clarify the parties' respective responsibilities for compliance with applicable Data Protection regulation.

2. Data Subject Rights

As a data subject, under the GDPR you have a number of rights. You can request to exercise these by contacting GIA.

Right	What it means
Right of Access (DSAR)	You can request access to your personal data and obtain a copy of it.
Right to Rectification	You can ask us to correct any inaccurate or incomplete personal data.
Right to Data Portability	You can request that your data is transferred to another organisation.
Right to Erasure	You can request deletion of your data when it is no longer necessary.
Right to Object	You can object to processing based on legitimate interests.
Right to Restrict Processing	You can request temporary suspension of processing in certain situations.
Right to Withdraw Consent	Where processing relies on consent, you can withdraw it at any time.

3. Processing your personal data overseas

As a global organisation, Experian teams including GIA, Compliance, Legal and HR operate across multiple countries and jurisdictions. To ensure that concerns can be investigated effectively, it may be necessary for personal data contained in reports to be transferred or accessed outside the EU, for example in the United Kingdom, North America, or Brazil. Where this is necessary, Experian ensures that such transfers of personal data are carried out in compliance with applicable data protection laws and with appropriate safeguards and security measures, which are designed to ensure a consistent level of protection across the Experian group and its service providers.

In all cases, we take appropriate steps to ensure that personal data is handled in accordance with our Global Information Security Policy and applicable legal and regulatory requirements.

Where third-party providers process personal data on our behalf, such processing is carried out under appropriate contractual arrangements and subject to strict confidentiality and security obligations. Further information on how such providers process personal data is available in their respective privacy notices.

4. Legal Bases for Processing

The categories of personal data processed in connection with concerns raised under this process are set out in Section 3.2 (“Categories of Personal Data”). The specific categories of data processed will depend on the nature of the concern, the information provided at the point of reporting, and any subsequent assessment, investigation, and follow-up activities.

Where a concern falls within the scope of applicable whistleblowing legislation, including the EU Whistleblowing Directive, Experian processes the relevant personal data in order to comply with its legal obligations. In such cases, the processing is necessary to receive, assess, investigate, and, where appropriate, take action in response to reported concerns, in line with applicable legal requirements.

Where a concern is assessed as falling outside the scope of such legislation — for example, where it relates primarily to an individual employment



grievance — Experian will process personal data on the basis of its legitimate interests. These include maintaining effective internal reporting mechanisms, ensuring appropriate escalation and resolution of concerns, and protecting the organisation, its employees, and other stakeholders.

In certain cases, the handling of a concern may require the processing of special category data. Where this occurs, such processing will be carried out only where necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment law, or otherwise in accordance with applicable data protection legislation.

Similarly, where the handling of a concern involves the processing of personal data relating to criminal offences or allegations, this will be undertaken only where permitted by applicable law and where necessary for purposes such as the prevention, detection, or investigation of unlawful acts, or for the establishment, exercise, or defence of legal claims.