

Last updated: August 2025

## Conduent Whistleblower Privacy Notice

This Whistleblower Privacy Notice ("**Notice**") applies to any individuals (excluding Conduent employees or others working for Conduent) such as job candidates, vendor and customer contacts, users of our website(s) and other members of the public who use our Hotline (see the Introduction section below). For the purposes of this Notice, this group is collectively referred to as "members of the public".

### Table of contents

1. [Introduction](#)
2. [Personal data we collect and process in connection with whistleblowing and our Hotline](#)
3. [How we use your personal data \(our purposes\) for whistleblowing and legal bases for processing it](#)
4. [Who we share your personal data with](#)
5. [How we keep your personal data secure](#)
6. [International data transfers](#)
7. [Data retention](#)
8. [Your data protection rights](#)
9. [Updates to this Privacy Notice](#)
10. [How to contact us](#)

We recommend that you read this Notice in full to ensure you are completely informed about how we collect, process, share and protect your personal data. However, if you only want to access a particular section of this Notice, then you can click on the relevant link above to jump to that section.

### 1. Introduction

---

This Notice explains how Conduent and its affiliates (collectively, "**Conduent**", "**we**", "**us**", "**our**") may process your personal data when you contact us as a whistleblower or make any other type of report of suspected violations of laws, company policies or other wrongdoing using Conduent's ethics hotline ("**Hotline**").

This Notice supplements our [Candidate / Recruitment Privacy Notice](#) and [Website Privacy Notice](#). For further information on sources of your personal data, how we process your personal data and your data protection rights, please see the relevant notice(s) to you.

Conduent provides the Hotline so that individuals can report ethics issues confidentially by email or telephone. This service is provided by Star Compliance (“**Star Compliance**”) on behalf of Conduent and is available to all members of the public (“**you**”).

Note that the laws of some countries do not permit reports to be made anonymously, however, your personal data will be treated confidentially and will only be disclosed as set out in this Notice or as otherwise required or permitted by applicable law or court order. If you do not report anonymously, either at your discretion or because anonymous reporting is not permissible under applicable law, please note that we may be required to disclose your identity to the subject of your report or as otherwise provided under applicable law.

We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law. If you have any comments or questions about this Notice, then please contact us using the contact details under the “[How to contact us](#)” heading below.

[Return to top](#)

## 2. Personal data we collect and process in connection with whistleblowing and our Hotline

---

If you make a report through the Hotline, unless it is anonymous, we may process personal data about you as described in the table below. We will also process personal data about other individuals when you name individuals in your report as being relevant to the matter you are reporting. For example, you may be reporting their behaviour, or the individual(s) may have witnessed an event you are reporting or otherwise be implicated.

Subsequent to reporting an issue, further information may be collected and processed about you, witnesses and/or other individuals implicated in the report for the purpose of investigating the incident. Some of this information may be collected from sources other than you such as witness evidence, background checks and testimonies. In each case, we will only do so where permissible and in accordance with applicable law.

The outcome of the investigation will also be recorded and that could involve documenting personal data about individuals, including regarding disciplinary or legal action taken and outcomes of that action.

Data Categories	Personal Data Description	Source
<b>Audio/Visual Data</b>	Voice recordings where you make a report to our telephone hotline.	<ul style="list-style-type: none"><li>• Automatic collection</li></ul>
<b>Communication Data</b>	Contact details and content of communications when you communicate with us through the Hotline or in communications such as email exchange or interview in relation to an investigation.	<ul style="list-style-type: none"><li>• Directly from you</li><li>• Automatic collection</li></ul>

<b>Contact Data</b>	Home and business address, personal and work telephone number, personal and work email addresses.	<ul style="list-style-type: none"> <li>• Directly from you</li> </ul>
<b>Ethics Reporting Data</b>	<p>Information reported to us, which may include personal data about yourself and other individuals such as those that have engaged in alleged misconduct, including (alleged) criminal activity or witnesses.</p> <p>Information collected in connection with an investigation, such as description of the alleged misconduct, witness statements and evidence gathered to ascertain the facts and circumstances.</p> <p>Conclusions of the investigation.</p>	<ul style="list-style-type: none"> <li>• Automatic collection</li> <li>• Directly from you</li> <li>• Third parties</li> </ul>
<b>Identity Data</b>	Name or alias, gender.	<ul style="list-style-type: none"> <li>• Directly from you</li> </ul>
<b>IT Data</b>	Information required to provide access to the Hotline electronically or by telephone (and information collected by / through those systems) such as telephone number, IP addresses, log files and login information. IT Data may also include, inferred location based on your IP address or activities, device identifiers associated with your computer or device, mobile carrier and related information, activity logs, and other information about activities you engage in on Conduent property, equipment, accounts, systems and networks.	<ul style="list-style-type: none"> <li>• Automatic collection</li> </ul>
<b>Security and Access Data</b>	Where an investigation takes place on our premises, such as conduct of interviews or meetings in connection with an investigation, closed-circuit television (CCTV) footage in public or common areas in our premises and near our premises (such as in car parking areas and in which case footage may include vehicle licence plates) may be collected. Other security and access data collected on our premises may also include other information obtained through electronic means such as security records (e.g. swipe card records, building entry / exit data to which Conduent may from time to time have access) and if you are visiting a premises in connection with an investigation, physical or electronic guest book information containing name, photograph, vehicle licence plate and person(s) you are visiting).	<ul style="list-style-type: none"> <li>• Automatic collection</li> <li>• Third parties (where used for CCTV, security and access systems)</li> </ul>

<b>Sensitive Personal Data</b>	Information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, genetic data, biometric data for the purposes of unique identification, trade union membership, information about your health (including mental health and vaccination status), disability, sexual orientation or sex life.	<ul style="list-style-type: none"> <li>• Directly from you</li> <li>• Third parties (e.g. from witnesses)</li> </ul>
--------------------------------	---	--

For information more generally on sources of personal data we collect and process about you, please see the relevant privacy notice(s) to you which can be accessed via the [“Introduction”](#) section of this Notice above.

[Return to top](#)

### 3. How we use your personal data (our purposes) for whistleblowing and legal bases for processing it

---

The following table provides more details on our whistleblowing related purposes for processing your personal data and the related legal bases for processing it.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
<b>Operating the Hotline and investigating reports made through the Hotline</b>	<i>Audio/Visual Data</i> <i>Communication Data</i> <i>Contact Data</i> <i>Ethics and Reporting Data</i> <i>Identity Data</i> <i>IT Data</i> <i>Security and Access Data</i> <i>Sensitive Personal Data</i>	<p>(a) <i>Necessary to comply with a legal obligation.</i></p> <p>Conduent operates the Hotline to comply with legal requirements. In the EU, the relevant laws are the Directive (EU) 2019/1937 on the Protection of Persons Who Report Breaches of Union Law as transposed into national law. In the UK, the relevant laws are the Public Interest Disclosure Act 1998.</p> <p>(b) <i>Where necessary for our legitimate interests.</i></p> <p>In some cases, reports may be made through the Hotline which fall outside of the EU and UK laws mentioned above. However, we may nevertheless wish to investigate and in which case would consider it necessary for our legitimate interests of investigating, and remedying conduct that may be harmful to us or others, including where it exposes us to civil or criminal liability or violates our codes of conduct or employee policies and procedures.</p>

		<p>In relation to Sensitive Personal Data (in addition to the above lawful basis):</p> <p>(a) <i>Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.</i></p> <p>(b) <i>Necessary for reasons of substantial public interest.</i></p>
<b>Legal claims</b>	<p><i>Audio/Visual Data</i></p> <p><i>Communication Data</i></p> <p><i>Contact Data</i></p> <p><i>Ethics and Reporting Data</i></p> <p><i>Identity Data</i></p> <p><i>IT Data</i></p> <p><i>Security and Access Data</i></p> <p><i>Sensitive Personal Data</i></p>	<p>(a) <i>Where necessary for our legitimate interests.</i></p> <p>Through the course of the investigation breaches of the law may be alleged or uncovered and in which case, we may need to process personal data collected in the course of the investigation for the legitimate interests of establishing, making or defending against legal claims.</p> <p>(b) <i>To establish, make or defend legal claims.</i></p> <p>We may need to process Sensitive Personal Data to establish, make or defend legal claims.</p>
<b>Compliance with reporting obligations to third parties</b>	<p><i>Audio/Visual Data</i></p> <p><i>Communication Data</i></p> <p><i>Contact Data</i></p> <p><i>Ethics and Reporting Data</i></p> <p><i>Identity Data</i></p> <p><i>IT Data</i></p> <p><i>Security and Access Data</i></p> <p><i>Sensitive Personal Data</i></p>	<p>(a) <i>Necessary to comply with a legal obligation.</i></p> <p>Please see above (at the 'Operating the Hotline' purpose) for description of applicable laws.</p> <p>(b) <i>Where necessary for our legitimate interests.</i></p> <p>Please see above (at the 'Operating the Hotline' purpose) for description of legitimate interests.</p> <p>In relation to Sensitive Personal Data (in addition to the above lawful basis):</p> <p>(a) <i>Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.</i></p> <p>(b) <i>Necessary for reasons of substantial public interest.</i></p>

[Return to top](#)

#### 4. Who we share your personal data with

---

We take care to allow access to personal data provided or otherwise collected in connection with our operation of the Hotline only to those who require such access to perform their tasks and duties. Within the Conduent group, this may include, for example, human resources, IT and security and legal.

It will also include our third-party providers, including our Hotline provider Star Compliance in connection with operating the Hotline, third party investigators and external legal advisors.

We may also need to disclose personal data to a competent law enforcement body, regulatory, government agency or court.

[Return to top](#)

## **5. How we keep your personal data secure**

---

We use appropriate technical and organisational measures to protect the personal data that we collect and process about you through the Hotline or in the course of an investigation.

[Return to top](#)

## **6. International data transfers**

---

As we operate internationally, in some cases, your personal data may be transferred to another Conduent group company located in another country to your place of residence. Specifically, personal data may be transferred in connection with an investigation to our legal and IT/IS teams including operating in India and the US. These countries may have data protection laws that are different to the laws of your country (and, in some cases, may not be as protective).

Our Hotline provider, Star Compliance operates globally. This means that when we collect your personal data through the Hotline we will process it in any of these countries.

Where we transfer your personal data to countries and territories outside of the European Economic Area and the UK, which have been formally recognised as providing an adequate level of protection for personal data, we rely on the relevant "adequacy decisions" from the European Commission and "adequacy regulations" (data bridges) from the Secretary of State in the UK. We transfer staff, contacts and customer personal data from the European Economic Area and the UK to countries from which our group of entities operates in reliance on the European Commission's adequacy decision for and the Secretary of State's adequacy regulations (where in place).

Where the transfer is not subject to an adequacy decision or regulations, we have taken appropriate safeguards to ensure that your personal data will remain protected in accordance with this Privacy Notice and applicable laws. The safeguards we use to transfer personal data are in case of both our group companies and third party service providers and partners, the [European Commission's Standard Contractual Clauses](#) as issued on 4 June 2021 under Article 46(2) using Module 1 for controller to controller

transfers, Module 2 for controller to processor transfers, Module 3 for processor to processor transfers and Module 4 for processor to controller transfers including the UK Addendum in each case for the transfer of data originating in the UK.

Our Standard Contractual Clauses entered into by our group companies and with our third party service providers and partners can be provided on request. Please note that some sensitive commercial information may be redacted from the Standard Contractual Clauses.

For transfers by Star Compliance from the European Economic Area and/or the UK to the US, Star Compliance rely on their Data Privacy Framework certification.

[Return to top](#)

## **7. Data retention**

---

We retain the personal data we collect from you through the Hotline or which we otherwise collect in connection with an investigations for as long as we have an ongoing legitimate business need to do so. For example, to comply with applicable legal requirements or for as long as statutory limitation periods for legal claims.

At the end of the period for which we need to keep your personal data, we will either delete or anonymise it or, if this is not possible (for example, because your personal data has been stored in backup archives), we will securely store and isolate it from any further processing until deletion is possible.

More specifically, we retain personal data in accordance with our Data Retention Policy.

For further information about our data retention periods please contact us using the contact details under the "[How to contact us](#)" heading below.

[Return to top](#)

## **8. Your data protection rights**

---

Individuals located in the UK and EEA have the following data protection rights. To exercise any of them see specific instructions below or contact us using the contact details provided under the "[How to contact us](#)" heading below.

- You may **access, correct, update or request deletion** of your personal data.

- You can **object to processing** of your personal data, ask us to **restrict processing** of your personal data or **request portability** of your personal data, (i.e. your data to be transferred in a readable and standardised format).
- If we have collected and processed your personal data with your consent, then you can **withdraw your consent** at any time by using the contact details provided under the “[How to contact us](#)” heading below. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent.
- You have the **right to complain to a supervisory authority** about our collection and use of your personal data. For more information, please contact your local supervisory authority. Contact details for supervisory authorities in Europe are available [here](#) and for the UK [here](#). Certain supervisory authorities may require that you exhaust our own internal complaints process before looking into your complaint.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

[Return to top](#)

## 9. Updates to this Privacy Notice

---

We may update this Notice from time to time in response to changing legal, regulatory, technical or business developments. When we update this Notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make.

You can see when this Notice was last updated by checking the “last updated” date displayed at the top of this Notice.

[Return to top](#)

## 10. How to contact us

---

If you have any questions or concerns about our use of your personal data, please contact using the following details:

**Brasil**

Livya Knoll  
Data Protection Officer  
DPO-Brasil@Conduent.com



**The Philippines**

Ronald Jomocan  
Data Protection Officer  
DPOPhilippines@Conduent.com

**European Economic Area**

Fieldfisher LLP  
Data Protection Officer  
ConduentDPO@conduent.com

**United Kingdom**

Fieldfisher LLP  
Data Protection Officer  
ConduentDPO@conduent.com

**All other countries**

Nicole Bearce  
Chief Privacy Officer  
DataPrivacy@Conduent.com

[Return to top](#)