

# **TCS Europe Policy – Whistle Blower**

---

VERSION 2.0

## Introduction

This Policy outlines the procedure for raising whistleblowing concerns or complaints in or related to an entity of the Tata Consultancy Services group of companies in Europe (each, “TCS Europe”). This is applicable for European Union and countries in Europe that have adopted the EU Whistleblowing Directive into their local laws (‘Europe’). This Policy is to be read in conjunction with the **TCS Global Policy - Whistle Blower** (referred to as ‘Global Whistle Blower Policy’) and country specific provisions on Whistleblower (if any) as specified in **ANNEXURE C**.

Along with the provisions specified in the Global Whistle Blower Policy, this Policy complies with the EU Whistleblowing Directive. This mandates TCS in Europe to have a separate internal and external reporting channel at the local level, and to give Whistleblowers the option to report through TCS internal channel.

For some European countries, the legislation offers additional protection to individuals who make disclosures about certain types of activities (such as corruption). Both TCS and TCS Europe are committed to complying with all relevant laws relating to whistleblowing and protected disclosures.

## Notes:

- a) *The provisions mentioned in this document are applicable in addition to the provisions mentioned in the Global Whistleblower Policy. In the event of a conflict between the provisions of the Global Whistleblower Policy, this Policy and local legal regulations the latter will supersede.*
- b) *Europe for the purpose of this document includes Austria, Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Sweden, Switzerland and Spain. Additional European countries will be added as and when there is a local TCS Europe entity operating in such country.*
- c) *For Switzerland and Norway, the EU Whistleblowing Directive is not applicable, however this Policy will also apply to TCS Europe operating in these countries, in addition to the local laws that apply with regards to whistleblowing in Switzerland and Norway.*

## Applicability

In addition to the provisions specified in the Global Whistle Blower Policy, this Policy is applicable to:

- Persons in managerial bodies of Tata Consultancy Services Limited (referred to as ‘TCS’) and its subsidiaries (collectively referred to as ‘Company’).
- All persons who have/had a (pre)-contractual relationship with Tata Consultancy Services (e.g. job applicant).

## Definitions

**"EU Whistleblowing Directive"** means the Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

**"Protected Disclosure"** is the communication of a violation, disclosing verifiable information and evidence of the Violation, made in good faith by the Whistleblower and as prescribed by the TCS Europe – Whistleblowing Procedure specified below in the document.

**"TCS Europe Trusted Person(s)"** is the person who is responsible for the assessment, investigation and reporting of any cases to any competent personnel as necessary that fall under the scope of this Policy.

**"TCS Europe Investigation Committee"** is the committee assigned by TCS Europe Trusted Person(s) to investigate a concern that falls under the scope of this Policy.

## Scope

In addition to the provisions specified in the Global Whistleblower Policy, whistleblowers may report breaches which may seriously harm the public interest of the European Union as defined in the EU Whistleblowing Directive in the areas of:

- public procurement,
- financial services – prevention of money laundering and terrorist financing,
- product safety,
- transport safety,
- protection of environment,
- nuclear safety,
- food and feed safety – animal health and welfare,
- public health,
- consumer protection,
- protection of privacy and personal data and security of network and information systems,
- breaches related to tax and financial services.
- breaches of employment law including violation of health & safety requirements.

## Reporting a Protected Disclosure

***Procedure to report a protected disclosure is available in detail in the*** Global Whistleblower Policy.

In addition, the provisions below are applicable as per the applicability of this Policy

1. There are three major channels through which Protected Disclosures may be made by whistleblowers:
    - Filing a report by means of a "physical meeting", which is to be scheduled within a reasonable timeframe from the date of request,
- OR,
- A whistleblower may also raise a concern with TCS Europe within the definition of this Policy through the TCS Europe Confidential Reporting System. They will have the option to raise a concern using the telephone service (please refer **ANNEXURE B** for the Europe country wise

phone numbers) or online through the TCS Europe Confidential Reporting System (please refer to section below on “Confidential Reporting System for more details on this).

2. A whistleblower, who provides their communication details will receive an acknowledgment of receipt of the Protected Disclosure within 7 days.
3. Protected Disclosure may be routed to the local authorities assigned for the whistleblowing after the internal reporting channel has been concluded without a satisfactory result for the whistleblower. The details of reporting to the local external channels are provided in Annexure A

*Note: The whistleblowing channel should not be used to challenge commercial decisions, nor as a mechanism for obtaining confidential business information. Any matters or concerns raised for such purposes and outside of the scope of this Policy, will be rejected.*

### Confidential Reporting System

TCS Europe has engaged an independent service provider (Convercent) to run its Confidential Reporting System. Stakeholders or third parties may raise concerns using **TCS Europe Confidential Reporting System**

- Individuals are requested to provide sufficient details to enable thorough investigation of their concerns. Concerns can be raised as per the individual’s preferred language.
- TCS Europe Trusted Person(s) and assigned investigators can only access details provided in the written report concern and will not have any access to the telephone number or email address from where it was made. TCS Europe Trusted Person(s) and assigned investigators will only contact the whistleblower through the independent service provider (Convercent), unless an alternate means of communication is agreed.

### Assessment and Investigations

Investigations will strictly follow TCS Europe policies and applicable legal regulations in the respective countries. The investigation and its outcome will be kept strictly confidential within TCS Europe Trusted Person(s) and assigned investigators. After the investigation is concluded, the outcome will be shared with the whistleblower as per applicable law and as necessary.

### Role of Trusted person(s) & Investigator(s)

#### a. Trusted person(s)

- i. The Trusted Person has been assigned to handle, assess and, where required, investigate whistleblowing concerns raised in the Europe Geography and defined in this Policy (to be read in conjunction with the Global Whistleblower Policy).
- ii. The Trusted Person reports into the geography Ethics Counselor and is supported for administrative purpose by dedicated Local Ethical Counselor, Europe as identified by the geography Ethics Counselor.

## **b. Investigators(s)**

If after the first assessment of the case where Trusted Person qualifies the concern to be covered under this Policy (including Country Annexure) and Trusted Person, in coordination with Geo Ethics Counselor decides the Whistleblower Concern is to be investigated, then:

- the Trusted Person can assign the respective Local Ethics Counselor(s) as Investigator(s).
  - The Trusted Person may also assign TCS Subject Matter Experts (SMEs) as Investigators, to be agreed with the geography Ethics Counselor, as Investigators, whose expertise is required for the investigation of the case.
- i. The investigator(s) assigned to the concern or case need to be highly competent in their roles and fully capable of executing their duties effectively and independently.
  - ii. Only once the Investigator(s) is/are selected for the case, they should receive an initial briefing from the Trusted Person and would be required to maintain confidentiality.

In case the Trusted Person identifies a conflict of interest, when Trusted Person and/or assigned Investigators handling the case or interacting with the whistleblowers and related stakeholders or otherwise see a conflict interest linked with the reported case, these persons will refrain from handling the case. For such cases, the Trusted Person will appoint a (new) Committee or member(s) in the Committee. For cases where a conflict of interest concerns the Trusted Person, the Geography Ethics Counselor will appoint the committee for investigation of the case concerned.

It will be ensured the SMEs will sign a Non-Disclosure Agreement (NDA) before they get involved.

## **c. Role of trusted Person and Investigator:**

- Advise on the interpretation of this Policy (to be read in conjunction with the Global Whistleblower Policy) and the Country Annexure (where applicable).
- Decide if concern is admissible under the Whistleblowing in Europe and it is to be considered to fall within the scope of this Policy and Annexure (where applicable)
- Guide Whistleblowers and TCS Europe in dealing with a concern or potential concern, acting as central point of contact for the whistleblower and any investigation
- Report the outcome of the report to the whistleblower.

The Trusted Person will be updated about a concern in the TCS Europe Confidential Reporting System or will receive a report based on the calls made to the TCS Whistleblowing line.

Whistleblowers are encouraged to use the internal channel first and may also raise concerns through the external channels available with the EU Member States in case of an unsatisfactory outcome. The list of external channels is attached as an Annexure ([ANNEXURE A](#)).

Throughout the investigation process, TCS Europe will ensure that:

- The investigation will be conducted autonomously and independently.
- The whistleblower is kept informed at reasonable intervals throughout the investigation.

The laws of the countries will be adhered to throughout the process, including the investigation, such as but not limited to data privacy laws. The applicable timeline and related requirements that are to be met (in comparison to the TCS Global Whistleblower Policy point under the section “Investigation”) are:

- The investigation outcome and the relevant decision on the same shall be issued within 90 calendar days of the receipt of the Protected Disclosure.
- The TCS Europe investigation committee and/or representative of the chairperson and/or TCS Europe Trusted Person(s) will communicate the outcome of the process to the concerned persons within the abovementioned timelines.

***Note:** Decisions taken by the TCS Europe Investigation Committee and/or the chairperson of the TCS Europe Investigation Committee, including interpretation of any of the clauses of the TCS Global Whistleblower Policy and this Policy, shall be concluded for and informed to all the persons concerned.*

### **Retention of documents**

All Protected Disclosures in writing or documented along with the results of the investigation relating to it shall be retained by the Company for a maximum period of seven years, or for a period as applicable under the laws of the respective country, starting from the date of issuance of the investigation outcome.

### **Rights and Obligations of Whistleblower and Stakeholders**

The identity and the information received from the whistleblower will be kept confidential as well to the extent possible given the legitimate needs of law and the investigation.

### **Confidentiality Obligations of the Whistleblower**

- Any information related to the concern will be considered confidential.
- Any disclosure of the same to third parties (with the exception of the maintenance of the whistleblowing channel kept with the third party as mentioned above) including media, press and social media (but excluding competent authorities and courts) is considered a serious violation of confidentiality unless the Protected Disclosure and the report to authorities has remained without sufficient timely response in the terms included in this Policy or in the applicable laws.

### **Amendment**

TCS reserves its right to amend or modify this Policy in whole or in part, at any time without assigning any reason whatsoever but without reducing its statutory obligations pursuant to the respective national implementation law of the EU Whistleblowing Directive. The revised Policy shall be uploaded onto the TCS website and on TCS Europe’s Internal policy portal as and when amended. If any country-specific requirements apply under whistleblowing laws in Europe they will be included in the Country Annexure.

## ANNEXURE A – TCS EUROPE - EXTERNAL CHANNELS (COUNTRY WISE)

Country	External reporting channel
Austria	Ministry of Justice
Belgium	Federal Ombudsman Vlaamse Ombudsman
Bulgaria	Bulgarian Commission for Anti-Corruption and Illegal Assets Forfeiture
Czech Republic	Ministry of Justice
Denmark	Data Protection Authority
Estonia	Ministry of Justice
Finland	Office of the Chancellor of Justice
France	Défenseur des Droits
Germany	Federal Office of Justice (Bundesamt für Justiz)
Hungary	Commissioner for Fundamental Rights
Italy	Autorità Nazionale Anticorruzione
Luxembourg	Whistleblower - Ministry of Justice // The Luxembourg Government (gouvernement.lu)
The Netherlands	Huis voor Klokkenluiders
Poland	Polish Commissioner for Human Rights ( <i>pol. Rzecznik Praw Obywatelskich</i> ). <a href="https://bip.brpo.gov.pl/en">https://bip.brpo.gov.pl/en</a> .
Portugal	Portuguese Ombudsman's Office Prosecutor General
Romania	Ministry of Justice
Slovakia	Whistleblower Protection Bureau i.e. Whistleblower Protection Office of Slovakia
Spain	La Autoridad Independiente de Protección al informante
Sweden	Ministry of Employment

**Non-EU countries to adhere to applicable rules and laws under the local legislation:** Norway and Switzerland

## ANNEXURE B - CONVERCENT HOTLINE PHONE NUMBERS - Europe Country wise

Country	Number
Austria	0800 281119
Belgium	0800 260 39
Bulgaria	0800 46038
Czech Republic	800 701 383
Denmark	8082 0058
Estonia	800 0100 431
Finland	0800 07 635
France	0805 080339
Germany	0800 181 2396
Hungary	212111440
Italy	800 727 406
Luxembourg	800-27-311
Netherlands	0-800-022-0441
Norway	800 24 664
Poland	00-800-111-3819 00-800-141-0213
Portugal	800 180 367
Romania	0-800-360-228
Slovakia	0 800 002 487
Spain	900 905460
Sweden	020 889 823
Switzerland	0800 838 835



## ANNEXURE C – COUNTRY-SPECIFIC

*Note: The content of this annexure covers country specific provisions arising from respective local legislation implementing EU Whistleblowing Directive. The specific provisions which may not be covered in this annexure will be honored and adhered to.*

### Austria

The protection under this Policy is extended in accordance with the Whistleblowing Protection Act (HSchG) to reports of violations of national law in relation to the criminal offense or corruption.

### Belgium

The scope under this Policy is extended in accordance with Belgium Whistleblower Act to also include breaches of the national law and breaches related to the internal market, including the rules on competition and State aid.

### Bulgaria

In deviation to this Policy and in accordance with the Whistleblowing Protection Act reports, violations committed more than two years ago cannot be received and will not be investigated.

### Denmark

The scope under this Policy is extended in accordance with the Danish Whistleblower Protection Act, which also includes breaches related to bribery, corruption, and sexual harassment.

### Finland

The scope under this Policy is applicable as per the Finnish Whistleblowing Act and is to include breaches of the Unions laws.

### France

- The requirements related to protection of the whistleblower (ref. TCS Global Policy – Whistleblower, chapter “Protection of whistleblower”) are extended to the facilitators of this whistleblower process, such as the TCS Europe Trusted Person(s), appointed investigators as well as union representatives who need to be protected from retaliation.
- The scope under this Policy is extended to the whistleblower reporting psychological or sexual harassment.

- In case the identity and the information received from the whistleblower needs to be disclosed due to the legitimate requirements of law and the investigation the whistleblower will be informed and consulted in advance.

### **Germany**

In deviation to period of Retention of documents under this Policy, the retention period shall be a maximum of 3 years from the date of closure of the case in accordance with the Law.

### **Hungary**

The scope under this Policy is extended in accordance with the Hungarian Whistleblower Protection Act XXV of 2023.

Investigation of the report may be waived if:

- a. The report was made by an unidentified whistle blower.
- b. the notification was not made by an authorized person as per the said Hungarian Act.

### **Netherlands**

The scope under this Policy is extended in accordance with the House of Whistleblowers Act, which also applies to situations of serious misconduct (in accordance with the Act).

### **Romania**

In deviation to the period of Retention of documents under this Policy, the retention period shall be a maximum of 5 years from the date the concern is registered in accordance with Law No. 361/2022.

### **Spain**

In accordance with Law 2/2023 the protection of people who report breaches of law and on combatting corruption the protection is in addition to whistleblowers extended to (in summary):

- The legal representatives of employees in the exercise of their functions of advising and supporting the informant.
- The legal entities in which the reporter has a significant shareholding.

### **Sweden**

In deviation to period of Retention of documents under this Policy, the retention period (in accordance with Swedish Whistleblowing Act) of personal data shared shall be a maximum of 2 years (from the date the concern is registered).

## **Poland**

The scope under this Policy is extended in accordance with Polish Whistleblower Act, including breaches concerning corruption, Polish State Treasury, local government or European Union financial interests.

The scope under this Policy does not cover breaches of Tata Code of Conduct and other internal procedures and/or employment laws, including health and safety breaches.

Trusted Person will engage with the Country HR Managers for any reported concerns to the extent which does not cause any conflict of interest.

In deviation to the retention period for any documents received as part of the reported concern under this Policy, the retention period shall be a maximum of 3 years after the end of the calendar year in which measures were implemented or after the completion of the proceedings initiated related to the concern and/or measures.