Global Privacy Policy

v.1.0. Public

Table of Contents

1. Purpose 3
2. Scope and Applicability 3
3. Definitions 3
4. Roles and Responsibilities 3
5. The Personal Data We Process 3
6. Our Data Protection Principles 4
7. Why We Process Personal Data — Purposes and Legal Bases 5
7.1 As Data Controller 5
7.2 As Data Processor 5
8. How we Share Personal Data and International Transfers 6
8.1 Sharing within the TP Group 6
8.2 Sharing with Third Parties 6
8.3 Sub-Processors 6
8.4 International Transfer Mechanisms 6
8.5 Website Cookies and Online Tracking 6
9. Your Rights as a Data Subject 7
9.1 How to Exercise Your Rights 8
10. Security – Protecting Personal Data 8
11. How Long We Keep Personal Data 9
12. Artificial Intelligence and Automated Decision-Making 9
13. Governance and Accountability 9
13.1 Privacy Leadership 9
13.2 Training 10
13.3 Updates to this Policy 10
14. Policy Violations 10
15. Key Contacts 10
16. TP Underlying Policies 11

1. Purpose

TP ("**TP**", "**we**", "**our**", "**us**") is committed to protecting the privacy and Personal Data of every person whose information TP handles, including its Workforce Members, Clients and their customers, and others who interact with its services around the world.

This Global Privacy Policy (the "**Policy**") sets the governing principles for all Personal Data Processing across TP. Detailed operational requirements are set out in the documentation of our BCRs and supporting policies referenced in **Section 16**.

2. Scope and Applicability

This Policy applies globally to:

- All Workforce Members of any TP Companies, in the performance of their duties.
- All Personal Data Processed by TP, whether as a Data Controller or as a Data Processor.

3. Definitions

Capitalized terms are defined in the *Global Glossary*.

4. Roles and Responsibilities

Where TP acts as a Data Processor on behalf of a Client, the Client's instructions and contractual terms govern alongside this Policy. This Policy does not limit any stricter obligations that may apply under local law — where applicable local law requires a higher level of protection for Personal Data, such law takes precedence over this Policy.

As Data Controller, TP determines how and why Personal Data is Processed.

As Data Processor, TP Processes Personal Data on behalf of Clients.

5. The Personal Data We Process

The Personal Data TP Processes varies depending on the services we provide and the role we play. As allowed under Applicable Data Protection Laws, categories of Personal Data Processed by TP may include, among others:

As Data Controller (as detailed in the BCR-C, Part 2, Section 1.1)

Personal Data relating to our Workforce Members, business and vendor contacts, and marketing and event contacts.

As Data Processor (on Client instructions and as detailed in the BCR-P, Part 2, Section 1.1)

The Personal Data varies by Client and type of service provided (for example, customer-care, visa-processing, interpretation and translation, and survey data).

Sources of Personal Data. TP collects Personal Data directly from individuals (for example, when Workforce Members are onboarded, or when someone contacts TP, applies for a role with a TP Company, attends a TP event, or uses a TP website); automatically through cookies and similar technologies when individuals

interact with TP's websites; from its Clients and their authorized representatives in connection with the services TP provides; and from Third Parties and publicly available sources where permitted by law, such as recruitment platforms, background-check providers, and references.

Sensitive Data. Sensitive Data (for example, health, biometric, racial or ethnic origin and criminal conviction data) is subject to additional safeguards as required by applicable law. TP Processes Sensitive Data only where there is an explicit lawful basis and appropriate protective measures are in place.

Children's Data. TP's services and websites are directed to businesses and adults, not to children. When acting as a Data Controller, TP does not knowingly collect Personal Data from children. If TP determines that it has collected a child's Personal Data without first obtaining any consent required under applicable law, TP will promptly take appropriate steps to delete the Personal Data or obtain the required consent, as applicable. Where TP Processes children's Personal Data solely on a Client's documented instructions as a Data Processor—for example, in connection with a Client service used by minors—the Client acts as the Data Controller and is responsible for establishing an appropriate lawful basis for Processing and obtaining any required parental or guardian consent. In such cases, TP Processes the Personal Data in accordance with its agreement with the Client and applies the safeguards required under that agreement.

If an individual believes that TP has collected a child's Personal Data while acting as a Data Controller, please contact TP at privacy@teleperformance.com.

6. Our Data Protection Principles

TP is committed to the following data protection principles and strives to ensure that its Processing reflects them:

Principle	What it means for TP
Lawfulness, Fairness & Transparency	We have a lawful basis for every Processing activity. We are open and honest about how and why we use Personal Data.
Purpose Limitation	We collect Personal Data for specified, explicit and legitimate purposes and do not Process it in ways incompatible with those purposes.
Data Minimization	We collect and retain only Personal Data that is adequate, relevant and necessary for its stated purpose.
Accuracy	We keep Personal Data accurate and up to date and correct or delete inaccurate data promptly.
Storage Limitation	We retain Personal Data only for as long as necessary, in accordance with our Global Data Retention Policy and applicable law.
Integrity & Confidentiality	We protect Personal Data against accidental loss, unauthorized access, disclosure, alteration or destruction using appropriate technical and organizational measures.

Accountability	We take responsibility for complying with these principles and can demonstrate that compliance through records, policies, training and audits.

7. Why We Process Personal Data — Purposes and Legal Bases

7.1 As Data Controller

When TP acts as a Data Controller and determines the purposes and means of Processing, it Processes Personal Data only where it has a lawful basis to do so under Applicable Data Protection Laws. Depending on the circumstances, TP may rely on one or more of the following lawful bases, among others, as recognized under Applicable Data Protection Laws:

- Contractual performance: Processing necessary to enter into or perform a contract, such as employing Workforce Members, paying suppliers, or establishing and managing business relationships.
- Legal obligation: Processing necessary to comply with applicable legal obligations, including employment, tax, anti-money laundering, health and safety, and other regulatory requirements.
- Legitimate interests: Processing necessary to pursue TP's legitimate business interests, such as protecting its business and systems, maintaining network and information security, preventing fraud, managing corporate communications and events, and developing, improving, and securing its products and services, provided those interests are not overridden by the rights and freedoms of the individuals concerned.
- Consent: Where required or appropriate under applicable law, TP will obtain the individual's consent before Processing Personal Data. Where Processing is based on consent, it may be withdrawn at any time, subject to applicable law.

Marketing Communications. Where TP sends marketing communications, it does so in accordance with applicable law and, where required, with the recipient's consent. Recipients may opt out of marketing communications at any time by using the unsubscribe link in the relevant communication or by contacting privacy@teleperformance.com.

7.2 As Data Processor

When TP Processes Personal Data on behalf of a Client, TP acts on the Client's instructions. TP does not determine the purposes or means of Processing Client Personal Data, except as necessary to provide the services or as otherwise required by applicable law. The categories of Personal Data Processed and the purposes of Processing are determined by the Client and vary depending on the Client's instructions, the services provided by TP, and Applicable Data Protection Laws. TP does not use Client Personal Data for any purposes beyond those permitted under its agreement with the Client or applicable law. TP implements appropriate technical and organizational controls to protect Client Personal Data in accordance with applicable law and the applicable Client agreement. If TP reasonably believes that a Client instruction would violate applicable law, TP will notify the Client before carrying out the Processing, unless prohibited by applicable law from doing so.

8. How we Share Personal Data and International Transfers

8.1 Sharing within the TP Group

TP Group entities share Personal Data with each other where operationally necessary, subject to the Intercompany Agreement and this Policy. Intragroup transfers from EEA/UK entities to non-EEA/UK entities are protected by the TP Group BCR-P (for Processor activities) and BCR-C (for Controller activities), approved by the CNIL and/or the UK BCRs approved by the ICO. TP provides jurisdiction-specific privacy notices and addenda that supplement this Policy where local law requires; individuals should refer to any notice or addendum applicable to their jurisdiction.

8.2 Sharing with Third Parties

TP may share Personal Data with Third Parties only where necessary and permitted under the Applicable Data Protection Laws and under appropriate safeguards:

- Third-Party Data Processors: vendors and service providers (non-TP) who Process data on TP's behalf under written contracts containing equivalent data protection obligations.
- Law enforcement and regulators: where required by applicable law or a binding court/authority order. TP will notify the Client and/or relevant EEA/UK Supervisory Authority before disclosing, unless legally prohibited from doing so.
- Business transfers: in the event of a merger, acquisition or sale of assets, Personal Data may be transferred subject to equivalent protections.

8.3 Sub-Processors

When TP engages a Sub-Processor or a Third-Party Data Processor not already approved by the Client, TP will notify the Client at least 30 days in advance via TP's Trust Center or in accordance with its agreement with the Client. Clients may object on documented compliance or security grounds. Sub-Processors and Third-Party Data Processors are bound by the same data protection obligations as TP under the ICA and applicable contracts.

8.4 International Transfer Mechanisms

TP uses approved cross-border transfer mechanisms for international data transfers, including the TP Group BCR-P and BCR-C, the European Commission's Standard Contractual Clauses (and, for the United Kingdom, the UK Addendum to the approved EU Binding Corporate Rules, or the International Data Transfer Agreement or Addendum), recognized adequacy decisions, and the equivalent safeguards required by other applicable laws. If Personal Data is shared with Third Parties, such Third Parties will have signed the relevant Data Protection Agreements which shall include all required terms under the Applicable Data Protection Laws and contracts.

8.5 Website Cookies and Online Tracking

TP's public websites, including TP.com, use cookies and similar technologies for purposes such as enabling core site functionality, measuring and improving site performance, and, where applicable, advertising. Where required by law, we obtain consent through a cookie banner before placing non-essential cookies, and we honor recognized browser-based opt-out signals (including Global Privacy Control) where it is required to do so. The cookies we use and the choices available to individuals are described in our Cookie

Notice and Website Privacy Notice and can be found at Data privacy information | TP. This Section addresses cookies and tracking technologies on TP's own websites, where TP acts as a Data Controller; it does not address cookies or tracking technologies on Client-operated properties for which TP acts only as a Data Processor.

9. Your Rights as a Data Subject

Individual privacy rights vary based on the Applicable Data Protection Law(s).

Your Right	What it means
Access	Request confirmation of whether TP Processes your Personal Data and request a copy of your Personal Data that TP holds, along with information on: • Purposes of Processing; • Categories of Personal Data; • Recipients, including transfers to non-EEA/UK countries and applicable safeguards; • Storage periods or criteria; • Your rights and how to exercise them; and • Whether decisions are based on automated Processing, including profiling.
Rectification	Ask TP to correct inaccurate or incomplete data.
Erasure	Ask TP to delete your data (subject to legal obligations) where: • Data is no longer necessary; • You withdraw consent (where applicable); • You object to Processing and no overriding legitimate grounds exist; • Processing is unlawful; and • Deletion is required by law.
Restriction	You may request that TP restricts Processing when: • Accuracy is contested; • Processing is unlawful and you prefer restriction over deletion; • Data is needed for legal claims; and • An objection request is pending assessment.
Portability	Receive your data in a structured, machine-readable format and request transfer to another Data Controller.
Object	Object to Processing based on legitimate interests or for direct marketing.
Automated decisions	Not be subject to decisions that significantly affect you based solely on automated Processing. With respect to such decisions, you may request human intervention, express your view, and/or contest the decision.
Withdraw consent	Withdraw consent at any time where Processing is consent-based.

9.1 How to Exercise Your Rights

To submit a request, contact TP at privacy@teleperformance.com or via our online privacy portal at Data privacy information | TP.

Where a Client's Personal Data is involved, TP may need to direct your request to the relevant Client, as they are the Data Controller for that data.

As a general matter, TP does not charge a fee for privacy rights requests. We may, however, charge a reasonable fee for manifestly unfounded or excessively repetitive requests.

TP responds within the timeframes required by applicable law. To protect your data, we may need to verify your identity before acting on a request, and we honor requests made by an authorized agent where the law allows. If TP declines a request, we will explain why and, where applicable law provides, you may appeal that decision or lodge a complaint with your local Supervisory Authority or other competent authority. Residents of the United States — and residents of other jurisdictions for which TP has published a supplemental privacy notice or addendum — should also review the applicable notice (for example, the U.S. State Privacy Notice) for additional rights and submission methods.

You may submit a privacy rights request through any of the following channels:

- By email: privacy@teleperformance.com;
- Via the online form available at Data privacy information | TP; or
- By post: Group Data Protection Officer, TP SE, 21–25 rue Balzac, 75008 Paris, France.

While you are encouraged to use these points of contact, you are not required to do so and may alternatively lodge a complaint directly with a competent Supervisory Authority or other appropriate authority, where applicable law permits.

10. Security – Protecting Personal Data

TP implements appropriate technical and organizational measures to protect Personal Data against accidental or unlawful access, loss, alteration, or disclosure. Measures are calibrated to the nature, scope, context, and severity of the Processing risk, and may include:

- Pseudonymization and encryption of Personal Data
- Multi-factor authentication and access controls
- Ongoing confidentiality, integrity, availability and resilience of systems
- Ability to restore access to data following an incident
- Regular testing, assessment and evaluation of technical measures
- Vendor and Sub-Processor security obligations
- Security incident response plan and Global Incident Response Team (GIRT)
- Mandatory annual privacy and security training for all Workforce Members

Security standards shall conform to local privacy and data protection laws and regulations, as well as to any contractual requirements.

11. How Long We Keep Personal Data

TP retains Personal Data only for as long as necessary to fulfill the purposes described in this Policy, comply with legal and regulatory obligations, resolve disputes, enforce agreements, or as otherwise permitted or required by applicable law. TP maintains retention schedules that reflect the nature and sensitivity of the data, the purposes for which it is Processed, applicable contractual commitments, legal requirements, and legitimate business needs.

Where TP Processes Personal Data on behalf of a Client, TP returns or securely deletes such data at the end of the applicable services in accordance with its contractual commitments, applicable law, and the Client's documented instructions. Where applicable law requires TP to retain Personal Data after the services have ended, TP will maintain the confidentiality of the data and Process it only to the extent required by law.

TP may anonymize or aggregate Personal Data so that it no longer identifies any individual and may retain and use such non-identifying information for legitimate business purposes, including analytics, benchmarking, research and development, improving the security, quality, reliability, and performance of its products and services, and developing, evaluating, and improving artificial intelligence and other technologies, as further described in Section 12 (Artificial Intelligence) and, where applicable, required or permitted by the relevant Client agreement.

Once Personal Data is no longer required for the purposes for which it was collected or retained, and no legal or other lawful basis for continued retention exists, TP securely deletes or anonymizes the data.

12. Artificial Intelligence and Automated Decision-Making

TP is committed to the responsible development and use of Artificial Intelligence (AI), guided by principles of safety, transparency, ethics and accountability. Where TP uses AI to Process Personal Data, it applies appropriate safeguards, and its Processing may involve a combination of automated and human methods. Where required by applicable law, TP will make it transparent when an individual is interacting with an automated system rather than a person.

TP does not knowingly make decisions that produce legal or similarly significant effects on an individual based solely on automated Processing.

TP does not use Personal Data to develop, train, or improve AI systems unless it has informed the affected individual or Client and obtained any authorization required by law, or unless the data has first been de-identified, anonymized, or aggregated so that it no longer identifies any individual. Where AI is used in connection with services TP provides to a Client, the applicable AI Addendum and Data Processing Agreement govern the permitted use of Client Personal Data.

13. Governance and Accountability

13.1 Privacy Leadership

TP has appointed a Group DPO who serves as the primary point of contact for the CNIL and other Supervisory Authorities. TP’s privacy program is led by senior privacy leadership and supported by a privacy network of local DPOs and Privacy, Risk and Compliance Officers (PRCOs) across TP Group entities worldwide.

13.2 Training

All Workforce Members who Process Personal Data must complete TP's annual privacy and data protection training. Workforce Members with higher privacy exposure receive additional, role-specific training. Completion is monitored by TP's internal privacy and training teams.

13.3 Updates to this Policy

This Policy is reviewed annually by the Global Privacy, Risk and Compliance Office and approved by the Group Chief Legal Officer. Material changes are communicated to all TP Group entities, to affected Clients, and to the CNIL annually (or in advance for changes that could affect the binding character of the BCRs). Changes to the public version are made accessible to Data Subjects. The CNIL is notified once a year of any changes or, where no changes have been made, of that fact.

14. Policy Violations

Failure to comply with this Policy may result in severe consequences for non-compliant Workforce Members and/or the Group, including criminal prosecution, monetary fines, and penalties. With respect to Workforce Members, non-compliance may also result in disciplinary action, up to and including termination.

All violations and Policy exceptions will be reported to the Governance & Risk Committee (GRC) by the Corporate Compliance Office, at least annually or where significant exposure risk is identified.

If you suspect, or know of a violation of this Policy, you must report it to your Line Manager, the Global Ethics Hotline at Teleperformance | Home (integrityline.com) (GEH), or the Global Incident Response Team (GIRT) at girt@teleperformance.com. Retaliation is not permitted against any Workforce Member who makes a report in good faith.

Where a deviation from this Policy is justified, an exception shall be requested by contacting the Global Privacy, Risk and Compliance Office via privacy@teleperformance.com.

15. Key Contacts

Key Contacts	
Group DPO (Privacy queries & DSARs)	privacy@teleperformance.com | Data privacy information | TP
Global Ethics Hotline	https://tp.integrityline.com/
Global Incident Response Team	GIRT@teleperformance.com
EMEA Privacy Office	EMEAPrivacyOffice@teleperformance.com
Lead Supervisory Authority (CNIL)	www.cnil.fr | +33 (0)1 53 73 22 22
UK Supervisory Authority (ICO)	www.ico.org.uk | 0303 123 1113

16. TP Underlying Policies

This Policy should be read in conjunction with TP's underlying policies and standards found on TP's website:

- BCR-C (Binding Corporate Rules for Controllers)
- BCR-P (Binding Corporate Rules for Processors)
- U.S. State Privacy Notice
- Website Privacy Notice
- Code of Conduct and Ethics