Teleperformance Group

Data Privacy Policy (BCRs)

External

February | 2025

DOCUMENT AND VERSION CONTROL

Ownership Roles	Read	Write	Delete
Global Privacy, Risk & Compliance Office	☒	☒	☒
Other Internal Users	☒	☐	☐

Version	Author	Remarks/ Changes	Reviewed by	Approved by	Date Approved
2.7	Alan Winters	Privacy Policy External	Nick Kirtley and Mark Jaffe	Leigh P. Ryan	10/22/2019
2.8	Charlotte Coffey/Hope Cameron-Douglas	Updated for UK leaving EU and formatting.	Sarah Godley and Nathan Coffey	Nathan Coffey	06/11/2021
2.9	Ariel Conrad Malimas	Annual review conducted - No changes made	Nathan Coffey	Sarah Godley (on Nathan Coffey behalf)	07/11/2022
3.0	Ariel Conrad Malimas	Updated position for Country Privacy Lead to Privacy, Risk and Compliance Officer Updated Section 2.2.1 – Right To Access to provide more clarity on Data Subjects obtaining a copy of their personal data.	Nathan Coffey Sarah Godley	Nathan Coffey	23/02/2023
4.0	Tiffany Fok Tong, Sara Nicole Churnside, Emily Chung Shui	Updated Definitions, Roles, links, and information throughout to provide further detail in line with EDPB recommendations.	Gilles Paoletti	Sarah Godley	12/01/2025

Owner	Global Privacy, Risk & Compliance Office
Document Type	Policy
Version	4.0
Status	Approved
Effective Date	12/01/2025
Classification	Teleperformance Public

NOTE: This is a CONTROLLED document. Any documents appearing in paper form should be checked against the TP Policy version.

Index

TP STANDARD

Part 1: Introduction

Definitions

"**Adequate Country**" means any country, territory or one or more specified sectors within that country, or organization that is located outside of the EEA/UK and is recognized by the European Commission for the EEA, or the ICO for the UK, as ensuring an adequate level of protection of Personal Data. The list of Adequate Countries for the EEA is available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

"**BCR**" means Binding Corporate Rules and constitutes a legal mechanism enabling transfers of Personal Data originating from or Processed in the EEA/UK within the Group.

"**BCR-C**" means the Controller Binding Corporate Rules (particularly Parts 1 and 2 of these BCRs).

"**Client**" means a third party to whom Teleperformance provides services described in a contract signed between Teleperformance and such Client. In this situation, the Client acts as a Data Controller in relation to the Processing of Personal Data by Teleperformance, which in turn acts as a Data Processor on behalf of such Client.

"**CNIL**" means *Commission Nationale de l'Informatique et des Libertés*, which is the French DPA, and the lead DPA for Teleperformance.

"**CPO**" means the Chief Privacy Officer.

"**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**DPA**" means Data Protection Authority (i.e., a privacy regulator).

"**DPO**" means the designated Data Protection Officer, when required by applicable laws and regulations.

"**Data Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller.

"**Data Subject**" means any natural person identified or identifiable by his/her Personal Data.

"**EEA**" means the European Economic Area and includes all member states of the European Union, as well as Iceland, Liechtenstein, and Norway.

"EEA/UK" means the European Economic Area and the UK.

"**Functional Privacy Lead**" means the primary point of contact between a global or regional function within Teleperformance for which he/she is responsible, and the Privacy Office.

"**Group**" means Teleperformance SE and any subsidiary that is wholly or partially owned, whether directly or indirectly, by Teleperformance SE.

"ICO" means Information Commissioner's Office, which is the UK DPA.

"Intercompany Agreement" or "**ICA**" means the contractual agreement between Teleperformance and its subsidiaries and affiliates wherein they abide by the conditions set forth in Teleperformance's BCR.

"**Personal Data**" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**Privacy Office**" means the Chief Privacy Officer and Regional Privacy Officers.

"Privacy, Risk and Compliance Officer" means the primary point of contact between the TP Company or local function for which he/she is responsible and the Privacy Office. The responsibilities of the Privacy, Risk and Compliance Officers are listed in Part 1, Section 5.2.1 of the Policy.

"**Process**" or "**Processing**", in relation to Personal Data, means any operation or set of operations which is performed on the Personal Data or sets of Personal Data, whether or not by automatic means, which includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making the Personal Data available, alignment or combination, restriction, erasure or destruction.

"**Profiling**" means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a Data Subject, in particular to analyze or predict aspects concerning that Data Subject's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

"**Sensitive Data**" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health, sex life or sexual orientation.

"**Sub-processor**" means a TP Company contracted by another TP Company, acting as a Data Processor, to Process Personal Data.

"**Regional Privacy Officers**" are individuals whose role and responsibilities are listed in Part 1, Section 5 of the Policy.

"**Teleperformance**" or "**TP Company/ies**" means any/all subsidiary/ies of the Group.

"**Third-Party Data Processor**" means a non-TP Company contracted by a TP Company to Process Personal Data.

"Workforce Members" means individuals that perform work or otherwise provide services for any Teleperformance Company, such as, but not limited to, employees, contractors, staffing agencies, and vendors.

Purpose

This policy ("the Policy") expresses the strong commitment of Teleperformance Group to respect and protect the privacy and Personal Data of every individual, including its Workforce Members, suppliers, customers, business partners, Clients and their respective end customers. Its purpose is to provide appropriate safeguards when the Group, or any of its TP Companies, Processes Personal Data.

In line with privacy and data protection laws and regulations applicable in EEA countries and the UK, the Policy also constitutes a legal mechanism (i.e., "Binding Corporate Rules") enabling international data transfers within the Group, whenever Teleperformance acts either as a Data Controller or a Data Processor, including when it transfers such Personal Data on behalf of a Client. When Personal Data is transferred within the Group on behalf of a Client, the Client remains responsible for (i) deciding whether the Policy provides appropriate safeguards for such transfers, and (ii) implementing other safeguards if it chooses not to rely on the Policy.

Scope

The Policy applies globally to all TP Companies.

Depending on the role of a TP Company in Processing, it shall apply the Policy as follows:

- When it Processes Personal Data as a Data Controller, it shall comply with Parts 1 and 2 of the Policy.
- Where it Processes Personal Data as a Data Processor on behalf of Teleperformance or another TP Company (which act as Data Controller), it shall comply with Parts 1 and 2 of the Policy; or
- When it Processes Personal Data as a Data Processor on behalf of a Client, it shall comply with Parts 1 and 3 of the Policy, as well as with the Client's instructions provided in the contract signed with such a Client.

Some TP Companies may act both as a Data Controller and a Data Processor on behalf of a Client, and hence shall comply with Parts 1, 2, and 3 of the Policy as appropriate.

The Policy sets global requirements which all TP Companies shall follow marked in black. "EEA/UK" and "BCR" requirements apply in addition to such global requirements. Requirements in the Policy marked in green apply in cases when such EEA/UK Personal Data are transferred to TP Companies in non-EEA/UK countries. Requirements applicable when the Personal Data under Processing are subject to laws and regulations applicable in EEA countries and the UK **and** when such EEA/UK Personal Data are transferred to TP Companies in non-EEA/UK countries are marked in dark blue.

No country-specific privacy policies are permitted for TP Companies based in EEA countries and the UK. Where country-specific privacy policies are developed for non-EEA/UK countries, they must reference this Policy and save to the extent, if any, mandated by applicable law must not have provisions that contradict with the applicable requirements in this Policy.

3.2 Conflict between the Policy and Local Laws and Regulations

- When local laws and regulations require a higher level of protection for Personal Data, they take precedence over the Policy. In addition, the specific requirements of the Policy apply only when local laws and regulations permit.

Part 2: Data Controller Activities

1. Processing of Personal Data

1.1 Purposes for Processing Personal Data

TP Companies acting as Data Controllers Process Personal Data for business-related purposes. The categories of Data Subjects and Personal Data and the purposes of Processing include, without being limited to, the following:

- **Employees, temporary staff, candidates, independent contractors, and trainees**, for human resources and personnel management processes, which may cover any type of Processing, and include recruitment, workforce planning, training and performance management, compensation and benefits, leave and benefits management, pay slip distribution, employee information and skill management, employee survey, exit interviews and process, and health and safety. Such Processing covers HR Personal Data, including, but not limited to, basic personal details (e.g., full name; age and date of birth); education, professional experience and affiliations (e.g., education and training history; languages; trade union membership); employee travel and expenses information (e.g., travel booking details; dietary requirements; passport and visa details); family, lifestyle and social circumstances (e.g., marital status; emergency contact details; religion or religious beliefs); basic HR details (e.g., job title, role; office location; start date); health, welfare and absence related (e.g., reason for absence; disability, access, special requirements details); employee training and performance related (e.g., disciplinary action, performance rating; call recording); financial details (e.g., bank account information; national insurance number; bonus payments); photographic, video and location information (e.g., CCTV images; tracking data); identification checks and background vetting (e.g., results of criminal checks; proof of eligibility to work); system access (e.g. access

logs, tracking information); account credentials (e.g., username, password, security questions).

- **Clients**, for Client relationship management, which may cover any type of Processing, and include developing new business relationships, sales, marketing, negotiating contracts, market research, managing existing business relationships, invoicing, Client services, handling enquiries, and to meet legal and regulatory obligations. Such Processing covers Client Personal Data, including, but not limited to, basic personal details (e.g., full name); photographic, video and location information (e.g., CCTV images); identification checks and background vetting (e.g., results of criminal checks; credit check related); system access (e.g. access logs, tracking information); account credentials (e.g., username, password, security questions).

- **Any other party**, for ensuring any other business operations, which may cover any type of Processing, and include supplier and vendor management, compliance, reporting, due diligence, buildings and facilities management, IT, customer surveys, and to meet legal and regulatory obligations. Such Processing covers third-party Personal Data including, but not limited to, basic personal details (e.g., full name); business activities (e.g., goods or services provided); financial details (e.g., bank account information); photographic, video and location information (e.g., CCTV images); identification checks and background vetting (e.g., results of criminal checks); system access (e.g. access logs, tracking information); account credentials (e.g., username, password, security questions).

1.2 Rules to follow while Processing Personal Data and Sensitive Data

Each TP Company and its Workforce Members shall observe the following principles while Processing Personal Data:

1.2.1 Fairness and Lawfulness

TP Companies shall always rely on a lawful basis for Processing Personal Data and Sensitive Data, in accordance with applicable local laws and regulations.

For the Processing of Personal Data subject to laws and regulations applicable in EEA/UK countries, TP Companies shall rely on one of the following grounds:

- The Data Subject has given his/her consent to the Processing of his/her Personal Data for one or more specific purposes.

- The Processing is necessary for the performance of a contract to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract.
- The Processing is necessary for compliance with a law or regulation applicable in an EEA/UK country to which the TP Company is subject.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the TP Company or in a third party to whom the Personal Data are disclosed; or
- The Processing is necessary for the purposes of the legitimate interests pursued by the TP Company or by the third party to whom the Personal Data are disclosed, except when such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

For the Processing of Sensitive Data subject to laws and regulations applicable in EEA/UK countries, TP Companies shall rely on one of the following grounds:

- The Data Subject has given his/her explicit consent to the Processing of his/her Sensitive Data for one or more specific purposes, except when prohibited by the laws and regulations applicable to the TP Company in an EEA/UK Country.
- The Processing is necessary for the purposes of carrying out the obligations and specific rights of the TP Company or of the Data Subject in the field of employment law and social security and social protection law, and insofar it is authorized by the laws and regulations applicable to the TP Company in an EEA/UK country, which laws and regulations provide for adequate safeguards.
- The Processing is necessary to protect the vital interests of the Data Subject or of another person, in each case when the Data Subject is physically or legally incapable of giving his/her consent;
- The Processing is carried out in the course of the legitimate activities, with appropriate safeguards, by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim, and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a third party without the Data Subject's consent;
- The Processing relates to Personal Data manifestly made public by the Data Subject;
- The Processing is necessary for the establishment, exercise or defense of legal claims, or whenever courts are acting in their judicial capacity; or

- The Processing of the Sensitive Data is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of laws and regulations applicable to EEA/UK countries, and when those Sensitive Data are Processed pursuant to contract with a health professional subject to the obligation of professional secrecy under laws and regulations applicable in EEA/UK countries, or by another person also subject to an equivalent obligation of secrecy.

For the Processing of Personal Data relating to criminal convictions and offences or related security measures subject to laws and regulations applicable in EEA/UK countries, TP Companies shall only Process such Personal Data under the control of an official authority, or when the Processing is authorized by laws and regulations applicable in EEA/UK countries providing for appropriate safeguards for Data Subjects' rights and freedoms.

When a Processing is based on a Data Subject's consent, TP Companies shall:

- Ensure that consent is freely given, specific, informed and an unambiguous indication of the Data Subject's wishes (by a statement or clear affirmative action) to agree to the Processing.
- Ensure that the Data Subject is able to withdraw his/her consent easily at any time and receives information of such ability prior to giving consent.
- Implement and maintain processes to record the giving and withdrawal of consent; and
- Ensure that if consent is given as part of a written declaration also concerning other matters, it is presented in a manner which is clearly distinguishable from other matters, in an intelligible form, using clear and plain language.

1.2 Transparency

Before collecting Personal Data, TP Companies shall provide Data Subjects with any information required by applicable laws and regulations, and at least with the identity and contact details of the Data Controller and of its representative, if any; the purposes of the Processing; the recipients or categories of recipients of the Personal Data; and the existence of Data Subjects' rights of access to, and to rectify, their Personal Data.

1.2.2.1 Personal Data Directly Obtained from the Data Subject

In addition, TP Companies shall provide Data Subjects with the information set out below in writing or by other means, including, when appropriate, in electronic form. It shall be provided in a concise, transparent, and easily accessible form, using clear and plain language:

- The contact details of the DPO, when applicable.
- The lawful basis for the Processing.
- The legitimate interest pursued by the TP Company or by a third party, when such interest provides the lawful basis for the Processing.
- In case of transfers to non-EEA/UK countries, the fact that the TP Company intends to transfer Personal Data to non-EEA/UK countries, the measures implemented to protect the Personal Data transferred, and the means by which a Data Subject can obtain a copy of them or where they have been made available.
- The period for which the Personal Data will be stored, or if not possible, the criteria used to determine this period.
- The existence of Data Subjects' rights to:
- Access to and erase Personal Data, restrict Processing, data portability, and to object to Processing. This objection right shall be explicitly brought to the Data Subject's attention, clearly and separately from any other information, when the Processing is based on the Data Controller's legitimate interest, or when Personal Data are Processed for direct marketing purposes.
- Withdraw consent at any time when it provides the lawful basis for the Processing of Personal Data or Sensitive Data. Such withdrawal shall not affect the lawfulness of the Processing carried out before the Data Subject's request for withdrawal of his/her consent; and
- Lodge a complaint before the applicable EEA/UK DPA.
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide them; and
- The existence of automated decision-making, including Profiling, and meaningful information about the logic involved, as well as the significance and envisaged consequences of such Processing for the Data Subject.

TP Companies intending to Process Personal Data for a purpose other than the initial purpose shall inform the affected Data Subjects prior to the further Processing with information on that other purpose, and with any relevant information as listed above.

1.2.2.2 Personal Data not Obtained Directly from the Data Subject

When Personal Data are not obtained directly from the Data Subject, the latter should be provided with the same information as listed in Section 1.2.2.1 above, as well as the categories of Personal Data concerned, the source from which the Personal Data originate, and whether the Personal Data came from publicly accessible sources.

Except when the Data Subject already has such information, it should be provided to him/her within 1 month of obtaining the Personal Data, having regard to the specific circumstances in which the Personal Data are Processed, or, if the Personal Data are to be used to communicate with the Data Subject to whom the Personal Data relates, at the latest at the time of first communication with that Data Subject, or, if a disclosure to a third party is envisaged, no later than the time when the Personal Data are first disclosed.

Such information is not required if its provision proves impossible or would involve a disproportionate effort, if collection or disclosure is expressly required by applicable laws and regulations, or if Personal Data shall remain confidential subject to an obligation of professional secrecy required by laws and regulations applicable in EEA/UK countries.

TP Companies intending to Process Personal Data for a purpose other than the initial one shall inform the affected Data Subjects prior to the further Processing with information on that other purpose, and with any relevant information as listed above.

When required by applicable laws and regulations, any notification or registration with a DPA shall be performed by TP Companies.

An up-to-date public version of the Policy and an up-to-date list of the TP Companies bound by the Policy shall be made easily accessible to Data Subjects on the Group's website https://www.tp.com/en-us/footer/privacy/

1.2.3 Purpose Limitation

TP Companies shall only collect Personal Data for one or more specified, explicit, and lawful purposes, and not further Process them incompatibly with those purposes.

1.2.4 Data Minimization and Accuracy

Personal Data shall be adequate, relevant, and not excessive in relation to the purposes for which the Personal Data are Processed.

Similarly, Personal Data shall be accurate and, where necessary, kept up to date; Teleperformance will exert reasonable effort to ensure that Personal Data that are determined to be inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without undue delay. It is the responsibility of the Data Subject to inform Teleperformance of any inaccuracy or update of his/her Personal Data. However, Teleperformance will exert reasonable effort to ensure its databases are as accurate and up to date as possible, including deleting inaccurate Personal Data.

1.2.5 Data Retention

Personal Data shall not be kept for longer than is necessary, and retention shall be in accordance with the following rules:

- The retention period during which Personal Data are kept shall be reviewed periodically.
- This retention period shall be adequate for the purpose/s of the Processing, and the Personal Data shall not be kept once the purpose/s has/have been accomplished; and
- Once they are no longer required, all Personal Data shall be deleted or anonymized in a secure manner ensuring protection from unlawful or wrongful access.

A BCR member acting as data importer, which ceases to be bound by the BCR-C may keep, return, or delete the personal data received under the BCR-C. If the data exporter and data importer agree that the data may be kept by the data importer, protection must be maintained in accordance with Chapter V GDPR.

1.2.6 Integrity and Confidentiality

Teleperformance Companies shall implement appropriate technical and organizational measures, as further specified.

2 Data Subjects' Rights Concerning their Personal Data

2.1 Data Subjects' Rights to Access, Correct, Erase, or Object.

Teleperformance commits that all Data Subjects should be provided with information on their third-party beneficiary rights, regarding the Processing of their Personal Data, and on the means to exercise those rights in accordance with applicable laws and regulations.

When required by applicable laws and regulations, TP Companies shall provide Data Subjects with the right to access their Personal Data Processed by the TP Company.

When required by applicable laws and regulations, TP Companies shall also provide Data Subjects with the ability to correct, without undue delay, their Personal Data when it is incomplete or inaccurate, including by means of providing a supplementary statement.

TP Companies shall adhere to the procedure referred to in Part 2, Section 10 of the Policy when responding to Data Subjects' requests to access, correct, erase, and object.

2.2.1 Right to Access

In relation to the right to access, Data Subjects shall be given access to the following:

- Confirmation as to whether the TP Company Processes Personal Data about that Data Subject.
- Explanation of the purposes of the Processing, the categories of Personal Data, and the recipients or categories of recipients to whom the Personal Data are disclosed (particularly recipients in non-EEA/UK countries) and the appropriate safeguards provided to such transfers.
- When possible, the period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period.
- A copy of their Personal Data undergoing Processing, and of any available information as to their source when the Personal Data are not obtained from the Data Subject.
- The existence of the right to request from the TP Company rectification or erasure of Personal Data, or restriction of Processing of Personal Data concerning the Data Subject, or to object to such Processing.
- The right to lodge a complaint with an applicable EEA/UK DPA; and
- When the TP Company makes decisions based solely on automated Processing of Personal Data, including Profiling, meaningful knowledge of the logic involved in such automatic Processing, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

TP Companies may only reject an access request when they can prove that:

- The TP Company is unable to verify the identity of the Data Subject.
- The Data Subject's right to such request is specifically limited by a law or regulation applicable in an EEA/UK country; or
- The request would impinge on the protection of the rights and freedoms of third parties, when redaction of the Personal Data and/or other measures to mitigate such effects are not reasonably feasible.
- The Data Subject is engaged in a litigation or other legal process with or relating to a Teleperformance Company, or there is a strong suspicion that the Data Subject will initiate litigation with a Teleperformance Company, in accordance with applicable laws and regulations.

2.2.2 Right to Erasure

TP Companies shall give Data Subjects the ability to request the erasure of their Personal Data without undue delay if:

- The Personal Data are no longer necessary in relation to the purpose(s) for which they were collected or otherwise Processed.
- The Data Subject withdraws consent on which the Processing is based, and there is no other lawful basis for the Processing.
- The Data Subject objects to Processing performed on the basis of the Data Controller's legitimate interests when there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing for direct marketing purposes.
- The Personal Data have been unlawfully Processed; or
- Personal Data shall be erased for compliance with laws and regulations applicable in EEA/UK countries to which the Data Controller is subject.

The Data Controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Data Controller shall inform the Data Subject about those recipients if the Data Subject requests it.

TP Companies may only reject an erasure request when they can prove that:

- The TP Company is unable to verify the identity of the Data Subject.
- The Data Subject's right to such request is specifically limited by a law or regulation applicable in an EEA/UK country.
- The request would impinge on the protection of the rights and freedoms of third parties, when redaction of the Personal Data and/or other measures to mitigate such effects are not reasonably feasible ("legal hold");
- The Processing is necessary for (i) exercising the right of freedom of expression and information; (ii) compliance with a legal obligation that requires Processing by laws and regulations applicable in EEA/UK countries to which the Data Controller is subject; or for (iii) the establishment, exercise, or defense of legal claims.

2.2.3 Right to Object

TP Companies shall provide Data Subjects with the ability to object at any time to the Processing of their Personal Data based on a TP Company's legitimate interests, including Profiling, unless that Processing is allowed by laws and regulations applicable in EEA/UK countries. When the objection is justified, the Processing shall cease, unless TP Companies can demonstrate compelling legitimate grounds for continuing the Processing that override the Data Subject's interests, rights, and freedoms, or for the establishment, exercise or defense of legal claims.

In addition, TP Companies shall provide Data Subjects with the ability to object at any time, on request and free of charge, to the Processing of their Personal Data for the purpose of direct marketing (including Profiling, to the extent that it is related to direct marketing). Such Processing shall stop as soon as reasonably possible.

TP Companies may only reject an objection request when they can prove that:

- The TP Company is unable to identify the Data Subject.
- The Data Subject's right to such request is specifically limited by a law or regulation applicable in an EEA/UK country; or
- The request would impinge on the protection of the rights and freedoms of third parties, when redaction of the Personal Data and/or other measures to mitigate such effects are not reasonably feasible.

2.2 Data Subjects' Right to Restrict Processing

TP Companies shall give Data Subjects the ability to restrict the Processing of their Personal Data, and to have their Personal Data segregated accordingly, if:

- The accuracy of the Personal Data is contested by the Data Subjects, for a period enabling the TP Company acting as a Data Controller to verify the accuracy of the Personal Data.
- The Processing is unlawful, and the Data Subjects oppose the erasure of the Personal Data and request the restriction of their use instead.
- The TP Company acting as a Data Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subjects for establishing, exercising, or defending legal claims; or
- The Data Subjects have objected to Processing carried out on the basis of the Data Controller's legitimate interests, pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subjects.

When the Processing is restricted, TP Companies may only Process Personal Data, except for storage:

- With the Data Subject's consent.
- For establishing, exercising, or defending legal claims.
- For protecting the rights of another natural or legal person; or
- For reasons of important public interest as defined under laws and regulations applicable in EEA/UK countries.

When TP Companies have restricted the Processing further to a Data Subject's request, they shall inform the Data Subject of such Processing restriction before it is lifted.

TP Companies may only reject a restriction request when they can prove that:

- The TP Company is unable to verify the identity of the Data Subject.
- The Data Subject's right to such request is specifically limited by a law or regulation applicable in an EEA/UK country; or
- The request would impinge on the protection of the rights and freedoms of third parties, when redaction of the Personal Data and/or other measures to mitigate such effects are not reasonably feasible.

TP Companies shall adhere to the procedure referred to in Part 2, Section 10 of the Policy when responding to Data Subjects' requests for restriction.

2.3 Data Subjects' Right for Data Portability

When the Processing is based on consent or on a contract, and carried out by automated means, TP Companies shall give Data Subjects the ability to request to

- Receive the Personal Data they have provided to a TP Company acting as Data Controller, in a structured, commonly used, and machine-readable format; and
- Transmit the Personal Data to another Data Controller without hindrance from the initial Data Controller, or to have them transmitted directly from one Data Controller to another, when technically feasible.

TP Companies may only reject a portability request when they can prove that:

- The TP Company is unable to identify the Data Subject;
- The Data Subject's right to such request is specifically limited by a law or regulation applicable in an EEA/UK country; or

- The request would impinge on the protection of the rights and freedoms of third parties, when redaction of the Personal Data and/or other measures to mitigate such effects are not reasonably feasible.

A Data Subject's request to portability of his/her Personal Data is without prejudice to his/her right to request erasure under Part 2, Section 2.2.2 of the Policy, and shall not adversely affect the rights and freedoms of others.

TP Companies shall adhere to the procedure set out in Part 2, Section 10 of the Policy when responding to Data Subjects' requests for data portability.

2.4 Automated Individual Decisions

TP Companies shall give Data Subjects the ability to object to any decision based solely on automated Processing of his/her Personal Data, including Profiling, which produces a legal effect concerning that Data Subject, or which otherwise significantly affects that Data Subject.

TP Companies may only reject such requests when they can prove that the decisions are:

- Necessary for entering or for the performance of a contract between the Data Subject and a TP Company acting as a Data Controller or based on the Data Subject's explicit consent. In such cases, TP Companies shall implement suitable measures to safeguard the Data Subjects' rights and freedoms and legitimate interests, at least the right to obtain human intervention from TP Companies, to express his/her point of view, and to contest the decision; or
- Authorized by laws and regulations applicable in EEA/UK countries, which also lay down measures to safeguard the Data Subject's rights and freedoms, and legitimate interests.

TP Companies shall only make decisions based solely on the automated Processing of Data Subjects' Sensitive Data if they have put in place suitable measures to safeguard the Data Subjects' rights and freedoms and legitimate interests, and when the Data Subject has given his/her explicit consent, or when the Processing is necessary for reasons of substantial public interest on the basis of laws and regulations applicable in EEA/UK countries.

TP Companies shall adhere to the procedure referred to in Part 2, Section 10 of the Policy when responding to Data Subjects' objections to decisions affecting them based on automated Processing, including Profiling.

3. Transfers of Personal Data

3.1 Transfers within the EEA or from the EEA to an Adequate Country

This describes the situation when a TP Company based in the EEA transfers Personal Data to one of the following:

- To another TP Company or third party also based in the EEA. An example would be a transfer of Personal Data by a TP Company in France to a TP Company in Italy; or
- To another TP Company or third party based in an Adequate Country. An example would be a transfer of Personal Data by a TP Company in Spain to a third party in Argentina.

Laws and regulations applicable in EEA countries authorize transfers of Personal Data between organizations based in the EEA, or from an organization based in the EEA to another organization based in an Adequate Country. Therefore, Teleperformance does not need to implement any additional measures in such cases.

3.2 Transfers from the EEA to a Non-Adequate Country

This describes the situation when a TP Company based in the EEA transfers Personal Data to another TP Company, or a third party located in a non-Adequate Country. An example would be a transfer of Personal Data by a TP Company in Ireland to a TP Company in the Philippines, or a TP Company in Germany being serviced by a third party in Turkey.

When an EEA TP Company transfers Personal Data to another TP Company located in a non-Adequate Country, such transfer is allowed insofar as that recipient TP Company entered into the Intercompany Agreement, has implemented the Policy and complies with its requirements, including with those marked with "**BCR**".

When an EEA TP Company acting either as a Data Controller or as a Data Processor on behalf of a TP Company acting as a Data Controller transfers Personal Data to a third party located in a non-Adequate Country, or to another TP Company which has not implemented the Policy (including the requirements of the Policy marked with "**BCR**"), the sending TP Company shall implement additional measures to protect the Personal Data transferred (e.g., by incorporating into the contract signed with the third party the appropriate Standard Data Protection Clauses issued by the European Commission or an EEA DPA), or shall ensure that the transfer matches with one of the conditions set forth by laws and regulations applicable in EEA countries (e.g., Data Subjects have explicitly given their consent to the transfer (after having been informed of the possible risks of such transfers for the Data Subject due to the absence of adequacy decision

and appropriate safeguards); or the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request).

When assessing the laws and practices of the third country which may affect the respect of the commitments contained in the policy, the BCR members have taken due account of the following elements regarding the specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

- purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials).
- types of entities involved in the processing (the data importer and any further recipient of any onward transfer).
- economic sector in which the transfer or set of transfers occur.
- categories and format of the personal data transferred.
- location of the processing, including storage.
- transmission channels used.

The Privacy team will inform all other BCR members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other BCR member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended. The data exporters have a duty to monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third countries to which the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

If this is not possible, the sending TP Company can operate a transfer if it is necessary for the purposes of compelling legitimate interests pursued by the TP Company acting as a Data Controller, provided that:

- The transfer or the set of transfers of Personal Data is not repetitive and concerns only a limited number of Data Subjects.
- The legitimate interests of the TP Company acting as a Data Controller are not overridden by the Data Subject’s interests or rights and freedoms.
- The TP Company acting as a Data Controller has assessed all the circumstances surrounding the transfer and on the basis of that assessment, has provided suitable safeguards with regard to privacy and data protection; and
- The TP Company acting as a Data Controller informs the applicable EEA DPAs and the Data Subjects of the transfer and the compelling legitimate interests.

Where the BCR member acting as data exporter, along with the Liable BCR member(s) and the relevant Privacy Function, assesses that the Policy, even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the relevant DPAs, it commits to7 suspend the transfer or set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended. The BCR member(s) acting as data importer(s) shall exercise their best efforts to implement further measures to mitigate any relevant risks assessed related to the transfer.

Teleperformance commits that following such a suspension, the BCR member acting as data exporter has to end the transfer or set of transfers if the BCR-C cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the BCR member acting as data exporter, be returned to it or destroyed.

In case of non-compliance, the data importer should promptly inform the data exporter if it is unable to comply with the policy. Where the data importer is in breach of the policy or unable to comply with them, the data exporter should suspend the transfer.
The data importer should, at the choice of the data exporter, immediately return or delete the personal data that has been transferred under the policy in its entirety, where:

- the data exporter has suspended the transfer, and compliance with this policy is not restored within a reasonable time, and in any event within one month of suspension; or
- the data importer is in substantial or persistent breach of the policy; or
- the data importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the policy.

The same commitments should apply to any copies of the data. The data importer should certify the deletion of the data to the data exporter.

Until the data is deleted or returned, the data importer should continue to ensure compliance with the BCR -C.

In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer should warrant that it will continue to ensure compliance with the BCR -C and will only process the data to the extent and for as long as required under that local law.

3.3 Transfers from Non-EEA/UK Countries to other Countries

This describes the transfer of Personal Data by a non-EEA/UK TP Company to another TP Company or third party based in another country. An example would be a transfer of Personal Data by a TP Company in Albania to a TP Company in China, or a TP Company in Mexico being serviced by a third party in Argentina.

Any transfer of Personal Data from a non-EEA/UK country to any other country shall be done with appropriate and reasonable protection, and in compliance with the laws and regulations applicable to the TP Company at the origin of the transfer, in particular, but not limited to, any legal requirement on transfers of Personal Data or pertaining to security.

When Personal Data transferred from the EEA/UK to non-EEA/UK TP Companies or third parties are further transferred to other non-EEA TP Companies, or third parties, the EEA/UK TP Company at the origin of the transfer shall ensure that such onward transfers comply with the rules set out in Part 2, Section 3.2 and 3.5.

3.4 Transfers within the UK or from the UK to an Adequate Country

This describes the situation when a TP Company based in the UK transfers Personal Data to one of the following:

- To another TP Company or third party also based in the UK; or
- To another TP Company or third party based in an Adequate Country. An example would be a transfer of Personal Data by a TP Company in the UK to a third party in France.

Laws and regulations applicable in UK authorize transfers of Personal Data between organizations based in the UK, or from an organization based in the UK to another organization based in an Adequate Country. Therefore, Teleperformance does not need to implement any additional measures in such cases.

3.5 Transfers from the UK to a Non-Adequate Country

This describes the situation when a TP Company based in the UK transfers Personal Data to another TP Company, or a third party located in a non-Adequate Country.

When a UK TP Company transfers Personal Data to another TP Company located in a non-Adequate Country, such transfer is allowed insofar as that recipient TP Company entered into

the Intercompany Agreement, has implemented the Policy and complies with its requirements, including with those marked with "**BCR**".

When a UK TP Company acting either as a Data Controller or as a Data Processor on behalf of a TP Company acting as a Data Controller transfers Personal Data to a third party located in a non-Adequate Country, or to another TP Company which has not implemented the Policy (including the requirements of the Policy marked with "**BCR**"), the sending TP Company shall implement additional measures to protect the Personal Data transferred (e.g., by incorporating into the contract signed with the third party the appropriate Standard Data Protection Clauses issued by or approved by the ICO), or shall ensure that the transfer matches with one of the conditions set forth by laws and regulations applicable in the UK (e.g., Data Subjects have explicitly given their consent to the transfer (after having been informed of the possible risks of such transfers for the Data Subject due to the absence of adequacy decision and appropriate safeguards); or the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request).

If this is not possible, the sending TP Company can operate a transfer if it is necessary for the purposes of compelling legitimate interests pursued by the TP Company acting as a Data Controller, provided that:

- The transfer or the set of transfers of Personal Data is not repetitive and concerns only a limited number of Data Subjects.
- The legitimate interests of the TP Company acting as a Data Controller are not overridden by the Data Subject's interests or rights and freedoms.
- The TP Company acting as a Data Controller has assessed all the circumstances surrounding the transfer and on the basis of that assessment, has provided suitable safeguards with regard to privacy and data protection; and
- The TP Company acting as a Data Controller informs the ICO and the Data Subjects of the transfer and the compelling legitimate interests.

4. Information Security

4.1 Security and Confidentiality

Teleperformance shall implement appropriate technical and organizational security measures to protect Personal Data from accidental loss, alteration, unauthorized disclosure or access, in

particular when the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the severity and likelihood of the risks represented by the Processing to Data Subjects' rights and freedoms, by the nature of the Personal Data to be protected, as well as the scope, context and purposes of the Processing. Such measures can include, as appropriate:

- The pseudonymization and encryption of Personal Data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services.
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; or
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

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

4.2 Personal Data Breach

In case of Personal Data breach, Teleperformance should implement an incident response plan.

Any personal data breach should be documented (comprising the facts relating to the personal data breach, its effects, and the remedial action taken), and the documentation should be made available to the relevant DPA upon request (see Articles 33 and 34 GDPR).

When the Personal Data breach is likely to result in a high risk to the Data Subjects' rights and freedoms, TP Companies shall also inform the affected Data Subjects of the breach without undue delay, describing in clear and plain language:

- The nature of the breach.
- The name and contact details of the DPO, when applicable, or other contact point from whom further information can be obtained.
- The likely consequences of the breach; and
- The measures taken or proposed to be taken by the TP Company to address the breach, including, when appropriate, measures to mitigate its possible adverse effects.

Communication to Data Subjects may not be required when:

- The TP Company has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the breach, particularly those that render the Personal Data unintelligible to any person who is not authorized to access it (e.g., encryption);
- The TP Company has taken subsequent measures to ensure that the high risk to the Data Subjects' rights and freedoms is unlikely to materialize; or
- It would involve disproportionate effort; in which case TP Companies shall issue a public communication or similar measure whereby affected Data Subjects are informed in an equally effective manner.

5. Relationship with Data Processors

When TP Companies acting as Data Controllers engage Third-Party Data Processors or Sub-processors, they shall conduct due diligence checks to evaluate that such Third-Party Data Processors or Sub-processors can provide sufficient guarantees in respect of the technical and organizational measures governing the envisaged Processing, such that the Processing will meet the security and confidentiality requirements set out in Part 2, Section 4.1 above.

In addition, TP Companies shall ensure that written contracts shall be in place.

6. Privacy by Design and Default

6.1 Privacy by Design

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the Processing, as well as the risks of varying likelihood and severity for the Data Subjects' rights and freedoms posed by the Processing, TP Companies shall, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organizational measures (e.g., pseudonymization) to enshrine privacy and data protection principles (e.g., data minimization) into prospective new or amended products, processes, technologies, systems, programs, and devices, when applicable, in an effective manner, and to integrate the necessary safeguards into the Processing of Personal Data.

6.2 Privacy by Default

- TP Companies shall implement appropriate technical and organizational measures to ensure that, by default, only Personal Data which is necessary for each specific purpose of Processing

are Processed. Such requirement applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility.

7. **Co-operation with DPAs**

It is the duty of all TP Companies and their Workforce Members to co-operate with and to respond diligently and appropriately to any inquiry or request, including an audit, by appropriate local DPAs and to comply with the advice given by such DPAs.

In addition, the applicable TP Company and the Privacy Office will co-operate with the applicable EEA/UK DPAs on any issue arising under the Policy and to comply with any decision or advice given by such DPAs.

Any dispute related to the Competent DPAs exercise of supervision of compliance with the policy will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural law. The BCR members agree to submit themselves to the jurisdiction of these courts.

8. Request and Complaint Handling

Teleperformance maintains an internal request and complaint handling procedure to allow Data Subjects to send requests on their rights pursuant to Part 2, Section 2 above, or to raise concerns about compliance with the Policy by any TP Company.

All TP Companies shall comply with Teleperformance Data Subjects Rights Procedure for Data Controller activities when handling Data Subjects' requests or complaints.

Data Subjects shall submit their requests on their rights to the local contact point identified in the applicable privacy and data protection notice, by submitting an on-line form at , https://www.tp.com/en-us/footer/privacy/ or shall submit their complaints about the Policy by sending an email to privacy@teleperformance.com.

No one shall be discriminated against for having submitted a request or complaint.

While Teleperformance encourages Data Subjects to use Teleperformance's dedicated complaint handling procedure, they have the right to lodge a claim directly with the applicable DPA and seek judicial remedies.

Teleperformance has the duty as the Data Controller to provide information on actions taken to the complainant without undue delay, and in any event within one month, by a clearly identified department or person with an appropriate level of independence in the exercise of their

functions. Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly.

9. Data Subjects' Third-Party Beneficiary Rights

Data Subjects whose Personal Data subject to laws and regulations applicable in EEA/UK countries were transferred to non-EEA/UK TP Companies or third parties on the basis of the Policy are entitled to enforce the requirements set forth in Part 1, Sections 2 (Purpose), 3 (Scope), and 4.3 (Conflict between the Policy and local laws and regulations), as well as Part 2 of the Policy, as third party beneficiaries in accordance with Part 2, Section 11 of the Policy.

This right covers the judicial remedies for any infringement of the rights guaranteed to Data Subjects, and the right to receive compensation.

Data Subjects can choose to lodge their claim before:

- The courts with jurisdiction over the EEA/UK TP Company at the origin of the transfer.
- The courts with jurisdiction over the place where the Data Subject has his/her habitual residence in the EEA/UK; or
- The EEA/UK DPA applicable for the EEA/UK country in which the Data Subject has his/her habitual residence, work, or where the alleged infringement took place.

Teleperformance has the duty to inform the Data Subjects about any update of the BCR-C and of the list of BCR member, e.g. by way of publishing the new version of this Policy without undue delay.

10. Liability

Teleperformance SE accepts responsibility for and agrees to take the necessary actions to remedy an infringement of the requirements contained in the Policy by non-EEA/UK TP Companies, and to pay compensation for any material or non-material damages resulting from such infringement. In this case, Data Subjects will have the same rights and remedies against Teleperformance SE as if an infringement had taken place in the EEA/UK.

Such liability extends only to Data Subjects whose Personal Data subject to EEA/UK laws and regulations applicable in EEA/UK countries were transferred to non-EEA/UK TP Companies or third parties in accordance with the Policy.

The burden of proof to demonstrate that Teleperformance is not responsible for any damage shall lie with Teleperformance SE. When Teleperformance SE can prove that the non-EEA/UK TP Company is not responsible for the act, it may discharge itself from any responsibility as described above.

11. Conflict Between the Policy and Local Laws and Regulations

TP Companies shall assess any judgment taken by a non-EEA/UK court or tribunal, or decision taken by a non-EEA/UK administrative authority requiring the transfer or disclosure of Personal Data which Processing is subject to laws and regulations applicable in EEA/UK countries, to ensure that such transfer or disclosure is done in compliance with laws and regulations applicable in EEA/UK countries.

The data importer will provide the BCR member acting as data exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the data importer is or becomes partially or completely prohibited from providing the data exporter with the aforementioned information, it will, without undue delay , inform the data exporter accordingly.

The data importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by the BCR -C and shall make it available to the Competent SAs upon request.

Notwithstanding the requirements provided in Part 1, Section 4.3 above, when a local law or regulation may prevent compliance with any requirement contained in the Policy or has substantial effect on the guarantees provided by the Policy, in particular those marked with "**BCR**", the affected TP Company shall promptly inform the Privacy Office, unless prohibited by a law enforcement, regulatory authority, state security body or court order (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In situations when non-compliance with the Policy would not have a substantial effect on the guarantees provided herein, local laws and regulations prevail.

The Privacy Office will decide on the appropriate actions to take to resolve the conflict, and when a non-EEA/UK local law or regulation applicable to a TP Company is likely to have a substantial adverse effect on the guarantees provided by the Policy, it will report the matter to the applicable EEA/UK DPA.

If Teleperformance receives a legally binding request for disclosure of the Personal Data Processed by a non-EEA/UK law enforcement, regulatory authority, state security body or court order, the following rules shall apply:

- Teleperformance will assess each request for disclosure on a case-by-case basis and inform the applicable EEA/UK DPA about the request, including information on the Personal Data requested, the requesting body, and the legal basis for disclosure, unless otherwise prohibited (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation);
- When suspension of the request and/or notification are prohibited (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), Teleperformance will use reasonable efforts to request a waiver of this prohibition in order to be able to communicate to the applicable EEA/UK DPA as much information as it can, and as soon as possible, and will keep evidence of the waiver request; and
- When such a waiver request has been denied, Teleperformance will annually provide general information on requests received (e.g. number of applications for disclosure, type of data requested, requester if possible) to the applicable EEA/UK DPAs.
- The data importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, transfers of Personal Data to any public authority cannot be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Part 3: Data Processor Activities

1. Processing of Personal Data

1.1 Purposes of Processing Personal Data

TP Companies acting on behalf of Teleperformance's Clients may Process Personal Data for the purpose of servicing those Clients. The nature and categories of the Personal Data, and the purposes of the Processing are determined by Teleperformance's Clients and will vary depending on both their instructions and the services provided by TP Companies.

Based on Teleperformance's business activities, the anticipated purposes, expected nature and categories of Personal Data covered by the Policy include, but are not limited to, the following:

- Clients' customers, as the Group's core business activities are the provision of outsourced customer relationship management services. Such Processing may cover any type of Processing, and any categories of Personal Data relating to Clients' customers, in accordance with Clients' instructions, which may include, but are not limited to, basic personal details

(e.g., full name, age and date of birth); business activities (e.g., services provided by the Clients); family, lifestyle and social circumstances (e.g., dependents, spouse, partner, family details; religion or religious beliefs; criminal convictions and offences); health related (e.g., details of physical and psychological health or medical condition); financial details (e.g., bank account information; national insurance number); photographic, video and location information (e.g., CCTV images); identification checks and background vetting (e.g., results of criminal checks; credit check related).

- Visa applicants, as TP Companies may provide outsourced services for visa applications. Such Processing may cover any type of Processing, and any categories of Personal Data relating to visa applicants, in accordance with Clients' instructions, which may include, but are not limited to basic personal details (e.g., full name; age and date of birth; passport details; biometric data); business activities (e.g., business activities of the Data Subject); family, lifestyle and social circumstances (e.g., dependents, spouse, partner, family details; religion or religious beliefs; criminal convictions and offences); health related (e.g., details of physical and psychological health or medical condition); financial details (e.g., bank account information; national insurance number); photographic, video and location information (e.g., photographic imaging); identification checks and background vetting (e.g., results of criminal checks; credit check related).
- Any Personal Data Processed in relation with outsourced interpretation or translation services, which can include, without being limited to: Clients' customer, patient, business partner, or public service user Personal Data. Such Processing may cover any type of Processing, and any categories of Personal Data Processed in the context of interpretation and translation services, which may include, but are not limited to, basic personal details (e.g., full name; age and date of birth; biometric data); education, professional experience and affiliations (e.g., education and training history; languages; trade union membership); employee travel and expenses information (e.g., travel booking details; dietary requirements; passport and visa details); family, lifestyle and social circumstances (e.g., marital status; emergency contact details; religion or religious beliefs); health and welfare related (e.g., disability, access, special requirements details; genetic data); financial details (e.g., bank account information; national insurance number); identification checks and background vetting (e.g., results of criminal checks; proof of eligibility to work).
- Customers and individuals participating in surveys, as TP Companies may provide outsourced customer survey services. Such Processing may cover any type of Processing, and any categories of Personal Data Processed in the context of conducting surveys, which may include, but are not limited to, basic personal details (e.g., age); family, lifestyle and social circumstances (e.g., family details; religion or religious beliefs); health, related (e.g., details of physical and psychological health or medical condition).

1.2 Rules to follow while Processing Personal Data

When acting on behalf of a Client, each TP Company and its Workforce Members shall respect the instructions regarding the Processing of Personal Data and the security and confidentiality measures as provided in the contract with each Client, and shall observe the following principles:

1.2.1 Assist Clients to comply with Laws and Regulations

TP Companies acting as Data Processors will reasonably assist Clients in complying with laws and regulations, such as by ensuring transparent Processing of Personal Data and data quality.

In particular, Clients shall be informed about Sub-processors and/or Third-Party Data Processors relevant for their respective Processing.

An up-to-date public version of the Policy and an up-to-date list of the TP Companies bound by the Policy shall be made easily accessible to Data Subjects on the Group's website https://www.tp.com/en-us/footer/privacy/.

When Clients rely upon the Policy for the transfers performed by Teleperformance on their behalf, Parts 1 and 3 of the Policy will be incorporated into the contract with such Clients.

1.2.2 Comply with the Clients' Instructions

TP Companies shall Process Personal Data only on behalf of the Clients, and in compliance with their instructions.

In particular, Teleperformance shall undertake any necessary measures as instructed by Clients in order to update, correct, delete or anonymize any Personal Data Processed on their behalf. Each Sub-processor and Third-Party Data Processor to whom the Personal Data have been disclosed shall be informed of such instructions and shall comply with them.

TP Companies shall comply with the Client's documented instructions, including with regard to transfers of Personal Data to a non-EEA/UK country, unless not required to do so by laws and regulations applicable in EEA/UK countries to which the TP Companies are subject. In such a case, TP Companies shall inform the Clients of that legal requirement before Processing takes place, unless the laws and regulations applicable in EEA/UK countries prohibit such information on important grounds of public interest.

If a TP Company is not in a position to comply with a Client's reasonable instructions, it shall promptly inform both the Global Privacy, Risk & Office and the Client, and Teleperformance will

try to accommodate the Client's instructions taking into consideration local laws and regulations applicable in EEA/UK countries and the Policy. If the Client reasonably rejects Teleperformance's attempts to accommodate the Client's instructions, and neither Teleperformance nor the Client can find a solution to accommodate the Client's instructions, Teleperformance will allow the Client to suspend, for a legitimate privacy and data protection reason in accordance with laws and regulations applicable in EEA/UK countries, the transfer of Personal Data impacted until the TP Company can comply with the Client's reasonable instructions, and/or terminate the specific portion of services impacted under the applicable work order or statement of work in accordance with the contractual remedies provided in the contract signed with that Client, but only to the extent such situation substantially disrupts Teleperformance's ability to provide services to that Client.

When the provision of services to a Client terminates, all Personal Data Processed on behalf of that Client by Teleperformance and any Third-Party Data Processor shall, at the choice of the Client and in accordance with the relevant terms of its contract with Teleperformance, be either safely returned (including all copies) to the Client, or destroyed (including all copies).. Such return or destruction should be done within a 90-day timeframe after the termination of the contract between the Client and Teleperformance, which can be extended with the CPO's agreement, depending on the timeframe agreed in that contract.

When laws and regulations require storage by Teleperformance of the Personal Data transferred, it shall inform the Client and warrant that it will guarantee the confidentiality of the Personal Data and will not actively process that Personal Data anymore.

1.2.3 Help Clients to handle Data Subjects' Requests

Teleperformance shall assist Clients with handling any requests from Data Subjects who exercise their rights, including requests to access, correct or delete their Personal Data in accordance with applicable laws and regulations.

In particular, TP Companies, as well as any Sub-processor and any Third-Party Data Processor, when relevant, will execute any appropriate technical and organizational measures, insofar as this is possible, when requested by the Clients, for the fulfilment of their obligations to respond to Data Subjects' requests for exercising their rights, including by providing any useful information in order to fulfil the requests.

When Teleperformance directly receives a request from a Data Subject, it will promptly communicate it to the relevant Client, in which case the latter remains responsible for handling the request, unless it has specifically authorized Teleperformance to do so. In such cases, Teleperformance shall follow the instructions contained in the Client's contract. The costs of

requests directly handled by Teleperformance shall be borne by the Client, except if provided otherwise in the contract signed with such Client.

1.2.4 Obtain Clients' Authorization to use Sub-Processors or Third-Party Data Processors

Teleperformance can use Sub-processors or Third-Party Data Processors only after notifying the Client, and if the latter has not objected to the use of such Sub-processor or Third-Party Data Processor within 30 days of receiving the notification, except if provided otherwise in the contract signed with such Client.

In the case of a Sub-processor, the latter shall Process Personal Data in accordance with the Client's instructions and Teleperformance's privacy and data protection obligations set forth in the contract signed between Teleperformance and the Client.

In the case of a Third-Party Data Processor, Teleperformance shall only appoint third parties who provide sufficient guarantees in respect of Teleperformance's commitments under Part 3 of the Policy. In particular, such Third-Party Data Processors shall commit by way of a contract or other legal act under laws and regulations applicable in EEA/UK countries to Process Personal Data in accordance with the Client's instructions and Teleperformance's privacy and data protection obligations set forth in the contract signed between Teleperformance and its Client, and to adduce appropriate technical and organizational measures to ensure appropriate protection having regard to Part 3, Section 3.1 of the Policy.

If the Client reasonably objects to the addition or replacement of a Sub-processor or a Third-Party Data Processor, Teleperformance will (i) offer not to progress with the change, or (ii) offer an alternative solution to the Client, including the use of another Sub-processor or Third-Party Data Processor. If the Client rejects the alternative solution offered by Teleperformance for a legitimate privacy and data protection reason in accordance with laws and regulations applicable in EEA/UK countries, the Client may terminate the specific portion of services impacted under the applicable work order or statement of work, in accordance with the contractual remedies provided in the contract signed with that Client.

2 Transfers of Personal Data

Transfers of Personal Data to Sub-processors and Third-Party Data Processors shall be done in accordance with Part 3, Section 1.2.4 of the Policy and the requirements set forth below.

2.1 Transfers within the EEA or from the EEA to an Adequate country

This describes the situation in which a Client or TP Company based in the EEA transfers Personal Data to one of the following:

- Client to TP Company (Processor or Sub-processor) based in the EEA or Adequate Country. An example would be a transfer of Personal Data by a Client in France to a TP Company (Sub-processor) in Italy, or Client in Germany to TP Company (Processor) in Canada.
- TP Company to a Sub-processor or Third-Party Data Processor also based in the EEA. An example would be a transfer of Personal Data by a TP Company in France to a Sub-processor in Italy; or
- TP Company to a Sub-processor or Third-Party Data Processor based in an Adequate Country. An example would be a transfer of Personal Data by a TP Company in Spain to a Third-Party Data Processor in Argentina.

Laws and regulations applicable in EEA countries authorize transfers of Personal Data between organizations based in the EEA, or from an organization based in the EEA to another organization based in an Adequate Country. Therefore, Teleperformance does not need to implement any additional measures in such cases.

2.2 Transfers from the EEA to a Non-Adequate Country

This describes the situation in which either a client transfers Personal Data to a TP Company (Processor or Sub-processor), or a TP Company based in the EEA transfers Personal Data to a Sub-processor, or a Third-Party Data Processor located in a non-Adequate Country. An example would be a transfer of Personal Data by a TP Company in Ireland to a Sub-processor in the Philippines, or by a TP Company in Germany to a Third-Party Data Processor in Turkey, or by a Client in Spain to TP Company in Colombia. .

When either a Client transfers Personal Data to a TP Company located in a non-Adequate Country (Processor or Sub-processor), or an EEA TP Company transfers Personal Data to a Sub-processor located in a non-Adequate Country, such transfer is allowed insofar as that recipient Sub-processor entered into the Intercompany Agreement, has implemented the Policy and complies with its requirements, including with those marked with "**BCR**".

When an EEA TP Company transfers Personal Data to a Third-Party Data Processor located in a non-Adequate Country, or to a Sub-processor which has not implemented the Policy (including the requirements of the Policy marked with "**BCR**"), the sending TP Company shall implement

additional measures to protect the Personal Data transferred (e.g., by incorporating into the contract signed with the Third-Party Data Processor the appropriate Standard Data Protection Clauses issued by the European Commission or an EEA DPA), or shall ensure that the transfer matches with one of the conditions set forth by laws and regulations applicable in EEA countries (e.g., Data Subjects have given their consent to the transfer; or the transfer is necessary for the performance of a contract between the Data Subject and the Client or the implementation of pre-contractual measures taken in response to the Data Subject's request).

If this is not possible, the sending TP Company can operate a transfer if it is necessary for the purposes of compelling legitimate interests pursued by the Client, provided that the transfer or the set of transfers of Personal Data is not repetitive and concerns only a limited number of Data Subjects; the legitimate interests of the Client are not overridden by the Data Subject's interests or rights and freedoms, the Client has assessed all the circumstances surrounding the transfer and on the basis of this document assessment, has provided suitable safeguards with regard to privacy and data protection, and the Client informs the EEA DPAs and the Data Subject of the transfer and the compelling legitimate interests.

2.3 Transfers from Non- EEA/UK Countries to other Countries

This describes the transfer of Personal Data by a non-EEA/UK TP Company to a Sub-processor or Third-Party Data Processor based in another country. An example would be a transfer of Personal Data by a TP Company in Albania to a Sub processor in China, or by a TP Company in Mexico to a Third-Party Data Processor in Spain.

Any transfer of Personal Data from a non-EEA/UK country to any other country shall be done with appropriate and reasonable protection, and in compliance with the laws and regulations applicable to the TP Company at the origin of the transfer, in particular, but not limited to, any legal requirement on transfers of Personal Data or pertaining to security.

When Personal Data transferred from the EEA/UK to non-EEA/UK Sub-processors or Third-Party Data Processors are further transferred to other non-EEA/UK Sub-processors or Third-Party Data Processors, the EEA/UK TP Company, or non-EEA/UK TP Company at the origin of the transfer shall ensure that such onward transfers comply with the rules set in Part 3, Section 2.2 and 2.5.

2.4 Transfers within the UK or from the UK to an Adequate Country

This describes the situation in which a Client or TP Company based in the UK transfers Personal Data to one of the following:

- Client to TP Company (Processor or Sub-processor) based in the UK or Adequate Country.

- TP Company to a Sub-processor or Third-Party Data Processor also based in the UK.
- TP Company to a Sub-processor or Third-Party Data Processor based in an Adequate Country.

Laws and regulations applicable in the UK authorize transfers of Personal Data between organizations based in the UK, or from an organization based in the UK to another organization based in an Adequate Country. Therefore, Teleperformance does not need to implement any additional measures in such cases.

2.5 Transfers from the UK to a Non-Adequate Country

This describes the situation in which either a Client transfers Personal Data to a TP Company (Processor or Sub-processor) located in a non-Adequate Country, or a TP Company based in the UK transfers Personal Data to a Sub-processor or a Third-Party Data Processor located in a non-Adequate Country.

When either a Client transfers Personal Data to a TP Company (Processor or Sub-processor), or a UK TP Company transfers Personal Data to a Sub-processor located in a non-Adequate Country, such transfer is allowed insofar as that recipient Sub-processor entered into the Intercompany Agreement, has implemented the Policy and complies with its requirements, including with those marked with "**BCR**".

When a UK TP Company transfers Personal Data to a Third-Party Data Processor located in a non-Adequate Country, or to a Sub-processor which has not implemented the Policy (including the requirements of the Policy marked with "**BCR**"), the sending TP Company shall implement additional measures to protect the Personal Data transferred (e.g., by incorporating into the contract signed with the Third-Party Data Processor the appropriate Standard Data Protection Clauses issued by or approved by the ICO), or shall ensure that the transfer matches with one of the conditions set forth by laws and regulations applicable in the UK (e.g., Data Subjects have given their consent to the transfer; or the transfer is necessary for the performance of a contract between the Data Subject and the Client or the implementation of pre-contractual measures taken in response to the Data Subject's request).

If this is not possible, the sending TP Company can operate a transfer if it is necessary for the purposes of compelling legitimate interests pursued by the Client, provided that the transfer or the set of transfers of Personal Data is not repetitive and concerns only a limited number of Data Subjects; the legitimate interests of the Client are not overridden by the Data Subject's interests or rights and freedoms, the Client has assessed all the circumstances surrounding the transfer and on the basis of this document assessment, has provided suitable safeguards with regard to

privacy and data protection, and the Client informs the ICO and the Data Subject of the transfer and the compelling legitimate interests.

3. Information Security

3.1 Security and Confidentiality

TP Companies shall implement appropriate technical and organizational security measures to protect Personal Data from accidental loss, alteration, unauthorized disclosure or access, in particular when the Processing performed on behalf of Clients involves the transmission of data over a network, and against all other unlawful forms of Processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the severity and likelihood of the risks represented by the Processing performed on behalf of Clients to Data Subjects' rights and freedoms, by the nature of the Personal Data to be protected, as well as the scope, context and purposes of the Processing. Such measures can include, as appropriate:

- The pseudonymization and encryption of Personal Data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; or
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

In addition, TP Companies shall comply with security and organizational measures which at least meet the requirements of the Client's applicable privacy and data protection laws and regulations.

3.2 Personal Data Breach

In case of Personal Data breach, Teleperformance should implement an incident response plan, in co-operation with the relevant Chief Information Officer, the Global Chief Information Security Officer, the Privacy, Risk and Compliance Officer, and the Privacy Office, which includes the following:

- **Breach Containment and Recovery** – Teleperformance shall use its best efforts to resolve the incident by applying a recovery plan and, when necessary, procedures for damage limitation.

- **Risk Assessment** – Teleperformance will assess associated risks, such as the adverse consequences for Data Subjects and the affected Client; seriousness of the breach; and risk of repetition.
- **Breach notification** - In accordance with and in the timelines provided by local laws and regulations, Teleperformance shall inform the affected Client, and any other relevant stakeholder (e.g., the police, or banks, as the case may be), about the Personal Data breach, when required under applicable law.
- **Process Evaluation** – An investigation will be conducted to determine the cause of the breach and evaluate the effectiveness of the response made. Policies and procedures will be addressed accordingly.

In case of Personal Data breach, TP Companies shall also promptly inform the Clients impacted by the Personal Data breach after becoming aware of it (no later than 72 hours), as well as the GIRT team and the Privacy Office, including when the breach concerns a Third-Party Data Processor servicing such Clients. In addition, Teleperformance shall ensure that Sub-processors and Third-Party Data Processors shall have the duty to inform the TP Companies acting as a Data Processor without undue delay after becoming aware of any breach, who in turn will promptly inform the Clients of such breach.

4. Co-operation with DPAs

It is the duty of all TP Companies to co-operate with and to respond diligently and appropriately to any inquiry or request, including an audit, by appropriate local DPAs. TP Companies shall notify the Privacy Office whenever they receive any requests from a DPA, and any subsequent communications will be managed by the Privacy Office.

In addition, the applicable TP Company and the Privacy Office will co-operate with the applicable EEA/UK DPAs on any issue arising under the Policy, and to comply with any decision or advice given by such DPAs.

1. Co-operation with Clients

Teleperformance, and any Third-Party Data Processor, when applicable and reasonable, will co-operate and assist Clients in complying with applicable privacy and data protection laws and regulations, including in implementing appropriate technical and organizational measures. Any requests from Clients shall be handled promptly and assistance provided to the extent reasonably possible.

2. Complaint Handling

When a Client reports a complaint from a Data Subject related to compliance with the requirements of Parts 1 and 3 of the Policy marked with "**BCR**" concerning the Processing of

his/her Personal Data by Teleperformance or a Third-Party Data Processor, and requests Teleperformance, to the extent agreed in the contract signed between Teleperformance and that Client, to directly handle it, Teleperformance will take all necessary steps to make sure that the Data Subject complaint is handled in accordance with the procedure described below.

When a Data Subject wishes to make a complaint related to compliance with the requirements of Parts 1 and 3 of the Policy marked with "**BCR**" concerning the Processing of his/her Personal Data by Teleperformance or a Third-Party Data Processor, but the Client has factually disappeared, ceased to exist in law or has officially become insolvent without any successor entity, such Data Subject can lodge a complaint directly with Teleperformance by sending an email to privacy@teleperformance.com.

The Privacy Office, Data Protection Officers and Privacy, Risk and Compliance Officers, when appropriate, shall handle the complaint in accordance with the following procedure:

- A Data Subject's identity shall be verified before assessing a complaint about the Policy. Additional forms of identification can reasonably be requested to verify a Data Subject's identity.
- Send an acknowledgment within one week of receipt of complaint to the Data Subject and inform him/her about the procedure and timelines to respond.
- Based on the information contained in the complaint, assess whether the complaint is justified, and investigate to understand the circumstances of the Processing subject to the complaint (e.g., extent of the infringement subject to a complaint);
- When the investigation reveals that the complaint is justified, implement relevant measures to resolve the infringement without undue delay and in any event not later than one month from receipt of the complaint; and inform the Data Subject of the result of the investigation and of the remediation measures implemented.
- When a substantive response to the complaint cannot be provided within one month because of the complexity and/or number of the complaints, notify the Data Subject of any extension of the period to respond, together with the reasons for delay, and commit to providing a response within a further two months period.
- When the investigation reveals that the complaint is not justified, inform the Data Subject of the result of the investigation; and
- No matter whether the complaint is justified or not, the Data Subject shall be informed that he/she may escalate the complaint to the CPO if he/she is not satisfied by the response received to his/her complaint.

While Teleperformance encourages Data Subjects to use the Client's dedicated complaint handling procedure (or Teleperformance's dedicated handling procedure) if the Client has

factually disappeared, ceased to exist in law or has officially become insolvent without any successor entity), they have the right to lodge a claim directly with the applicable DPA and seek judicial remedies.

Any communication and any action taken by Teleperformance further to a Data Subject's complaint shall be provided free of charge, save that a reasonable fee may be charged if complaints are manifestly unfounded or excessive, in particular because of their repetitive character, in which case Teleperformance shall bear the burden of demonstrating the manifestly unfounded or excessive character of the complaints.

Teleperformance may refuse to act on complaints when:

- They are manifestly unfounded or excessive, in particular because of their repetitive character, and Teleperformance can demonstrate the manifestly unfounded or excessive character of the complaints.
- Processing does not require identification, and Teleperformance can demonstrate they are not in a position to verify the identity of a Data Subject; or
- The right of the Data Subject is expressly restricted by laws and regulations applicable in EEA/UK countries.

3. Data Subjects' Third-Party Beneficiary Rights

Subject to Part 3, Section 9.1 of the Policy, Data Subjects whose Personal Data subject to laws and regulations applicable in EEA/UK countries were transferred to non-EEA/UK TP Companies or third parties on the basis of the Policy, are entitled to directly seek a remedy against Teleperformance in respect of infringements of Part 1, Sections 3 (Scope) and 4.3 (Conflict between the Policy and local laws and regulations), as well as Part 3 of the Policy.

Subject to Part 3, Section 9.1 of the Policy, when Data Subjects whose Personal Data subject to laws and regulations applicable in EEA/UK countries were transferred to non-EEA/UK TP Companies or Third-Party Data Processors in accordance with the Policy, are not able to bring a claim against the Client, because it has factually disappeared, ceased to exist in law or has become insolvent without any successor entity, Data Subjects are entitled to seek a remedy in respect of infringements of Part 1, Sections 2 (Purpose limitation), 3 (Scope), and 4.3 (Conflict between the Policy and local laws and regulations), as well as Part 3 of the Policy.

Those Data Subjects' rights cover the judicial remedies for any infringement of the rights guaranteed to Data Subjects and the right to receive compensation.

Data Subjects can choose to lodge their claim before:

- The courts with jurisdiction over the EEA/UK Client or TP Company at the origin of the transfer;
- The courts with jurisdiction over the place where the Data Subject has his/her habitual residence in the EEA/UK; or
- The EEA/UK DPA responsible for the EEA/UK country in which the Data Subject has his/her habitual residence, work, or where the alleged infringement took place.

4. Liability

9.1 Towards Data Subjects

Subject to Part 3, Section 8, first paragraph of the Policy, Teleperformance SE accepts responsibility for and agrees to take the necessary actions to remedy an infringement of the requirements contained in the Policy by non-EEA/UK TP Companies and to pay compensation for any material or non-material damages resulting from such infringement. In this case, Data Subjects will have the same rights and remedies against Teleperformance SE as if an infringement had taken place in the EEA/UK.

Subject to Part 3, Section 8, second paragraph of the Policy, when the Client has factually disappeared, ceased to exist in law or has officially become insolvent without any successor entity, Teleperformance SE accepts responsibility for and agrees to take the necessary actions to remedy an infringement of the requirements contained in the Policy by non-EEA/UK TP Companies or non-EEA/UK Third-Party Data Processors, and to pay compensation for any material or non-material damages resulting from such infringement. In this case, Data Subjects will have the same rights and remedies against Teleperformance SE as if the infringement had taken place in the EEA/UK.

Such liability extends only to Data Subjects whose Personal Data subject to laws and regulations applicable in EEA/UK countries were transferred to non-EEA/UK TP Companies or non-EEA/UK Third-Party Data Processors in accordance with the Policy.

Teleperformance SE may not rely on an infringement by another TP Company or a Third-Party Data Processor of its obligations in order to avoid its own liabilities.

When the TP Company and the Client involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation, for the entire damage, directly from the TP Company.

When Teleperformance SE can prove that neither a non-EEA/UK TP Company nor a non-EEA/UK Third-Party Data Processor is responsible for the act, or if the act results from the Client, it may discharge itself from any responsibility as described above.

9.2 Towards Clients

The Policy will be made legally enforceable by Clients which rely on the Policy for the transfers by Teleperformance on their behalf through a specific reference to it in the contract with Clients. Subject to any provisions contained in a contract between Teleperformance and a Client, a Client shall have the right to enforce Parts 1 and 3 of the Policy against any TP Company for infringements caused by such TP Company servicing this, Client.

In addition, Teleperformance SE shall be responsible for any damage arising out of an infringement of:

- Parts 1 and 3 of the Policy or of the contracts signed with Clients by non-EEA/UK TP Companies; or
- The written contract signed with a non-EEA/UK Third-Party Data Processor, in accordance with Part 3, Section 1.2.4 of the Policy.

The Client shall have the right to judicial remedies and the right to receive compensation.

The burden of proof to demonstrate that Teleperformance is not responsible for any damage shall lie with Teleperformance SE. When Teleperformance SE can prove that the non-EEA/UK TP Company or non-EEA/UK Third-Party Data Processor is not responsible for the act, it may discharge itself from any responsibility as described above.

Teleperformance SE or any TP Company's liability is limited to infringements of the Policy and of a written contract signed with a non-EEA/UK Third-Party Data Processor, in accordance with Part 3, Section 1.2.4 of the Policy.

5. Conflict Between the Policy and Local Laws and Regulations

TP Companies shall assess any judgment taken by a non-EEA/UK court or tribunal, or decision taken by a non-EEA/UK administrative authority requiring the transfer or disclosure of Personal Data which Processing is subject to laws and regulations applicable in EEA/UK countries, to ensure that such transfer or disclosure is done in compliance with laws and regulations applicable in EEA/UK countries.

Notwithstanding the requirements provided in Part 1, Section 4.3 above, when an existing or future local law or regulation may prevent compliance with any requirement contained in the Policy, in particular those marked with "**BCR**", or with any reasonable instructions of the Clients, the affected TP Company shall promptly inform the Privacy Office, unless when prohibited by a law enforcement, regulatory authority, state security body or court order (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In situations when non-compliance with the Policy would not have a substantial effect on the guarantees provided herein, local laws and regulations prevail.

The Privacy Office will decide on the appropriate actions to take to resolve the conflict and will report all EEA matters to the EEA DPA applicable to the Client and to the CNIL and will report all UK matters to the DPA applicable to the Client and to the ICO.

In addition, the Client will be promptly informed of such risk of non-compliance with the Policy or the Client's instructions. Teleperformance will use reasonable efforts to offer an alternative solution to the concerned Client to solve the conflict in a reasonable period of time. If the Client rejects the alternative solution offered by Teleperformance for a legitimate privacy and data protection reason in accordance with laws and regulations applicable in EEA/UK countries, the Client will be entitled to suspend the transfer of the specific Personal Data impacted by this non-compliance until the TP Company can provide an adequate alternative solution, and/or terminate the specific portion of services impacted by this non-compliance under the applicable work order or statement of work in accordance with the contractual remedies provided in the contract signed with that Client, but only to the extent such conflict substantially disrupts Teleperformance's ability to provide services to that Client.

If Teleperformance receives a legally binding request for disclosure of the Personal Data Processed on behalf of a Client by a non-EEA/UK law enforcement, regulatory authority, state security body or court order, the following rules shall apply:

- The Client shall be promptly informed, unless otherwise prohibited (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation) or agreed with the Client;
- In any case, Teleperformance will assess each request for disclosure on a case-by-case basis and commits to putting the request on hold for a reasonable period of time in order to notify both the EEA/UK DPA applicable to the Client and the CNIL or ICO as applicable prior to the disclosure to the requesting body, and provide them with information on the request, the requesting body, and the legal basis for disclosure unless otherwise prohibited (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation);

- When suspension of the request and/or notification to the applicable EEA/UK DPAs are prohibited (e.g., prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), Teleperformance will use reasonable efforts to request a waiver of this prohibition in order to be able to notify both the EEA/UK DPA applicable to the Client and the CNIL or ICO as applicable, and will keep evidence of the waiver request; and
- When such a waiver request has been denied, Teleperformance will annually provide general information on requests received (e.g. number of applications for disclosure, type of data requested, requester if possible) to the above-mentioned EEA/UK DPAs.

tp.com