Teleperformance

Transforming Passion into Excellence

Teleperformance Group Data Privacy Policy

Document Control

Approved on: 03/12/2018
Effective Date:05/25/2018

Version: 2.6

TP Standard
Part 1: Introduction

Part 1: Introduction

1 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 and is recognized by the European Commission as ensuring an adequate level of protection of Personal Data. Adequate Country includes any further adequacy decision by the European Commission such as the EU-U.S. Privacy Shield. The list of Adequate Countries is available at:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

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

"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 your 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 your Personal Data.

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

"DPA" means a privacy or data protection authority.

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

"Data Subject" means any natural person identified or identifiable by his/her Personal Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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.

"EEA" means the European Economic Area and includes all member states of the European Union, as well as Iceland, Liechtenstein, and Norway.
"Group" means Teleperformance SE and any subsidiary that is wholly or partially owned, whether directly or indirectly, by Teleperformance SE.

"Local Privacy Lead" means the primary point of contact between the TP Company or local function for which he/she is responsible and the Privacy Office.

"Personal Data" means any information relating to a Data Subject, as defined herein above.

"Privacy Office" means the Chief Privacy Officer, and the three Senior Vice Presidents of Privacy.

"Process" or "Processing", in relation to Personal Data, means any operation or set of operations which is performed on your 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 your Personal Data available, alignment or combination, restriction, erasure or destruction.

"Profiling" means any form of automated processing of your Personal Data consisting of the use of your Personal Data to evaluate certain personal aspects relating to you, in particular to analyze or predict aspects concerning your 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 engaged by a TP Company acting as a Data Processor on behalf of a Client.

"SVPP" means Senior Vice President of Privacy.

"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.

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

2 Purpose

This policy ("the Policy") expresses the strong commitment of Teleperformance Group to respect and protect your privacy and Personal Data, whether you are part of our employees, suppliers, customers, business partners, Clients or their respective end customers. Its purpose is to provide appropriate safeguards when the Group, or any of its TP Companies, Processes your Personal Data.

In line with privacy and data protection laws and regulations applicable in EEA countries, 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 are 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.

3 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; 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, 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. "EEA" and "BCR" requirements apply in addition to such global requirements. Requirements in the Policy marked with "EEA" apply when your Personal Data under Processing are subject to laws and regulations applicable in EEA countries. Requirements in the Policy marked with "BCR" apply in cases when your EEA Personal Data are transferred to TP Companies in non-EEA countries.

4 Conflict between the Policy and local laws and regulations

When local laws and regulations require a higher level of protection for your 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

Part 2: Data Controller activities

I Processing of your Personal Data

1.1 Purposes for Processing your Personal Data

TP Companies acting as Data Controllers Process your 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:

(1) 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); account credentials (e.g., username, password, security questions).

(2) 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).

(3) 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).

1.2 Rules to follow while Processing your Personal Data and Sensitive Data

Each TP Company and its employees shall observe the following principles while Processing your Personal Data:

1.2.1. Fairness and lawfulness

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

EEA & BCR

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

- You have given your consent to the Processing of your Personal Data for one or more specific purposes;
- The Processing is necessary for the performance of a contract between you and the Data Controller, or in order to take steps at your request, prior to entering into a contract;
- The Processing is necessary for compliance with a law or regulation applicable in an EEA country to which the TP Company is subject;
- The Processing is necessary to protect your vital interests or those 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 your 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 your Personal Data are disclosed, except when such interests are overridden by your interests or fundamental rights and freedoms.

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

• You have given your explicit consent to the Processing of your Sensitive Data for one or more specific purposes, except when prohibited by the laws and regulations applicable to the TP Company in an EEA Country;
• The Processing is necessary for the purposes of carrying out your obligations and specific rights or those of the TP Company 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 country, which laws and regulations provide for adequate safeguards;
• The Processing is necessary to protect your vital interests or those of another person, in each case when you are physically or legally incapable of giving your 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 your Personal Data are not disclosed to a third party without your consent;
• The Processing relates to Personal Data you manifestly made public;
• 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 your 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 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 countries, or by another person also subject to an equivalent obligation of secrecy.

EEA & BCR

For the Processing of your Personal Data relating to criminal convictions and offences or related security measures subject to laws and regulations applicable in EEA 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 countries providing for appropriate safeguards for your rights and freedoms.

When a Processing is based on your consent, TP Companies shall:

• Ensure that your consent is freely given, specific, informed and an unambiguous indication of your wishes (by a statement or clear affirmative action) to agree to the Processing;
• Ensure that you are able to withdraw your consent easily at any time, and that you receive information of such ability prior to giving consent;
• Implement and maintain processes to record the giving and withdrawal of your consent; and
• Ensure that if your 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.

1.2.2. Transparency

Before collecting Personal Data, TP Companies shall provide you 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 your Personal Data; and the existence of your rights of access to, and to rectify your Personal Data.

1.2.2.1 Personal Data directly obtained from you

In addition, TP Companies shall provide you 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:

EEA & BCR

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

EEA & BCR

TP Companies intending to Process your Personal Data for a purpose other than the initial purpose shall inform you 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 your Personal Data are not obtained directly from you, you 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 your Personal Data originate, and whether your Personal Data came from publicly accessible sources.

If you have not already received such information before, you should receive it within 1 month of obtaining your Personal Data, having regard to the specific circumstances in which your Personal Data are Processed, or, if your Personal Data are to be used to communicate with you, at the latest at the time of first communication with you, or, if a disclosure to a third party is envisaged, no later than the time when your 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 your Personal Data shall remain confidential subject to an obligation of professional secrecy required by laws and regulations applicable in EEA countries.

TP Companies intending to Process your Personal Data for a purpose other than the initial one shall inform you 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 this Policy and an up-to-date list of the TP Companies bound by the Policy shall be made easily accessible to you on the Group's website http://www.teleperformance.com/en-us/privacy-policy/.

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

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

It is your responsibility to inform Teleperformance of any inaccuracy or update of your Personal Data. However, Teleperformance will exert reasonable effort to ensure its databases are as accurate and up-to-date as possible, including deleting your inaccurate Personal Data.

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

2 Your rights concerning your Personal Data

2.1 Data Subjects' rights to access, correct, erase, or object

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

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

TP Companies shall adhere to the procedure provided in Annex 1 of the Policy when responding to your requests to access, correct, erase, and object.

EEA & BCR

2.1.1 Right to access

You shall be given access to the following:
• Confirmation as to whether the TP Company processes your Personal Data;
• Explanation of the purposes of the Processing, the categories of Personal Data, and the recipients or categories of recipients to whom your Personal Data are disclosed (particularly recipients in non-EEA countries) and the appropriate safeguards provided to such transfers;
• When possible, the period for which your Personal Data will be stored, or, if not possible, the criteria used to determine that period;
• Communication of your Personal Data which are undergoing or have undergone Processing, and of any available information as to their source when your Personal Data are not obtained from you;
• The existence of your right to request from the TP Company rectification or erasure of your Personal Data, or restriction of Processing of your Personal Data, or to object to such Processing;
• The right to lodge a complaint with an applicable EEA DPA; and
• When the TP Company makes decisions based solely on automated Processing of your 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 you.

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

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

2.1.2 Right to erasure

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

EEA & BCR

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

When your Personal Data that are subject to your request for erasure have been made public by the TP Company acting as a Data Controller, it shall, having regard to available technology and cost of implementation, inform other Data Controllers which are Processing your Personal Data of your request to erase any links to, or copies or replication of, those Personal Data.

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

• The TP Company is unable to verify your identity;
• Your right to such request is specifically limited by a law or regulation applicable in an EEA country;
• Your request would impinge on the protection of the rights and freedoms of third parties, when redaction of your Personal Data and/or other measures to mitigate such effects are not reasonably feasible; or
• 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 countries to which the Data Controller is subject; or for (iii) the establishment, exercise or defense of legal claims.

2.1.3 Right to Object

EEA & BCR

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

In addition, you have the right to object at any time, on request and free of charge, to the Processing of your 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 a request when they can prove that:

• The TP Company is unable to verify your identity;
• Your right to such request is specifically limited by a law or regulation applicable in an EEA 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 Your right to restrict Processing

You have the right to restrict the Processing of your Personal Data, and to have your Personal Data segregated accordingly, if:

• You contest the accuracy of your Personal Data, for a period enabling the TP Company acting as a Data Controller to verify the accuracy of your Personal Data;
• The Processing is unlawful and you oppose the erasure of your Personal Data and request the restriction of their use instead;
• The TP Company acting as a Data Controller no longer needs your Personal Data for the purposes of the Processing, but you require them for establishing, exercising or defending legal claims; or
• You 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 yours.

When the Processing is restricted, TP Companies may only Process your Personal Data, with the exception of storage:

EEA & BCR

• With your 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 countries.

When TP Companies have restricted the Processing further to your request, they shall inform you 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 your identity;
• Your right to such request is specifically limited by a law or regulation applicable in an EEA country; or
• Your request would impinge on the protection of the rights and freedoms of third parties, when redaction of your Personal Data and/or other measures to mitigate such effects are not reasonably feasible.
TP Companies shall adhere to the procedure provided in Annex 1 of the Policy when responding to your requests for restriction.

2.3 Your right for data portability

When the Processing is based on your consent or on a contract, and carried out by automated means, you have the right to request to:

• Receive the Personal Data you have provided to a TP Company acting as Data Controller, in a structured, commonly used and machine-readable format; and
• Transmit your 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:

EEA & BCR

• The TP Company is unable to identify you;
• Your right to such request is specifically limited by a law or regulation applicable in an EEA country; or
• Your 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.

Your request to portability of your Personal Data is without prejudice to your right to request erasure under Part 2, Section 2.1.2 of the Policy, and shall not adversely affect the rights and freedoms of others.

TP Companies shall adhere to the procedure provided in Annex 1 of the Policy when responding to your requests for data portability.

2.4 Automated individual decisions

You have the right to object to any decision based solely on automated Processing of your Personal Data, including Profiling, which produces a legal effect concerning you, or which otherwise significantly affects you.

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

EEA & BCR

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

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

TP Companies shall adhere to the procedure provided in Annex 1 of the Policy when responding to your objections to decisions affecting you 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 your 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 your 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 your Personal Data by a TP Company in Spain to a third party in Argentina.

EEA & BCR

Laws and regulations applicable in EEA countries authorize transfers of your 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 your Personal Data to another TP Company or a third party located in a non-Adequate Country. An example would be a transfer of your 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 your Personal Data to another TP Company located in a non-Adequate Country, such transfer is allowed insofar as that recipient TP Company 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 your 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 your 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., you have explicitly given your consent to the transfer (after having been informed of the possible risks of such transfers for you due to the absence of adequacy decision and appropriate safeguards); or the transfer is necessary for the performance of a contract between you and the Data Controller or the implementation of pre-contractual measures taken in response to your request).

EEA & BCR

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 your 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 your 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 you and the applicable EEA DPAs of the transfer and the compelling legitimate interests.

3.3 Transfers from non-EEA countries to other countries

This describes the transfer of your Personal Data by a non-EEA TP Company to another TP Company or third party based in another country. An example would be a transfer of your 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 Spain.

Any transfer of your Personal Data from a non-EEA 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 your Personal Data or pertaining to security.

BCR

When your Personal Data transferred from the EEA to non-EEA TP Companies or third parties are further transferred to other non-EEA TP Companies or third parties, the EEA TP Company at the origin of the transfer shall ensure that such onward transfers comply with the rules set in Part 2, Section 0 above.

4 Information Security

4.1 Security and Confidentiality

Teleperformance shall implement appropriate technical and organizational security measures to protect your 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 your rights and freedoms, by the nature of your 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 your 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 your 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.

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

- The nature of the breach;
- The name and contact details of the SVPP and/or 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.

EEA & BCR

Communication to you 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 your 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 your 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 you are informed in an equally effective manner.

5 Relationship with Data Processors

EEA & BCR

When TP Companies acting as Data Controllers engage other 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 and shall stipulate any statutory data protection requirements.

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 your 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 your Personal Data.

6.2 Privacy by Default

TP Companies shall implement appropriate technical and organizational measures to ensure that, by default, only your Personal Data which are necessary for each specific purpose of Processing are Processed. Such requirement applies to the amount of your Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, by default, your Personal Data shall not be made accessible to an indefinite number of natural persons without your intervention.

7 Co-operation with DPAs

It is the duty of all TP Companies and their employees 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.

BCR

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

8 Request and Complaint handling

Teleperformance maintains an internal request and complaint handling procedure to allow you to send requests on your 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 adhere to the procedure provided in Annex 1 of the Policy when handling your requests or complaints.

BCR

You shall submit your requests on your rights to the local contact point identified in the applicable privacy and data protection notice, or by sending an email to privacy@teleperformance.com, and shall submit your complaints about the Policy by sending an email to privacy@teleperformance.com.

No one shall be discriminated against on the basis of submitting a request or complaint.

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

9 Your third-party beneficiary rights

When your Personal Data which Processing is subject to laws and regulations applicable in EEA countries were transferred to non-EEA TP Companies or third parties on the basis of the requirements of the Policy, you have the right to enforce the requirements set forth in Part 1, Sections 2 (Purpose), 3 (Scope), and 4 (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 10 of the Policy.

BCR

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

You can choose to lodge your claim before:

- The courts with jurisdiction over the EEA TP Company at the origin of the transfer;
- The courts with jurisdiction over the place where you have your habitual residence in the EEA; or
- The EEA DPA applicable for the EEA country in which you have your habitual residence, work, or where the alleged infringement took place.

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 TP Companies, and to pay compensation for any material or non-material damages resulting from such infringement. In this case, you will have the same rights and remedies against Teleperformance SE as if an infringement had taken place in the EEA.

BCR

Such liability extends only if your Personal Data which Processing is subject to EEA laws and regulations applicable in EEA countries and were transferred to non-EEA 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 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 court or tribunal, or decision taken by a non-EEA administrative authority requiring the transfer or disclosure of your Personal Data which Processing is subject to laws and regulations applicable in EEA countries, in order to ensure that such transfer or disclosure is done in compliance with laws and regulations applicable in EEA countries.

Notwithstanding the requirements provided in Part 1, Section 4 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).

EEA & BCR

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 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 DPA.

If Teleperformance receives a legally binding request for disclosure of your Personal Data Processed by a non-EEA 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 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);

EEA & BCR

• 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 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 DPAs.

In any case, transfers of your 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 activitie

Part 3: Data Processor activities

I Processing of your Personal Data

1.1 Purposes of Processing Personal Data

TP Companies acting on behalf of Teleperformance's Clients may Process your Personal Data for the purpose of servicing those Clients. The nature and categories of your 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:

1. 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).

2. 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).

3. 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).

4. 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 your Personal Data

When acting on behalf of a Client, each TP Company and its employees shall respect the instructions regarding the Processing of your 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 your 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 http://www.teleperformance.com/en-us/privacy-policy/.

BCR

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 your 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 your Personal Data have been disclosed shall be informed of such instructions and shall comply with them.

EEA & BCR

TP Companies shall comply with the Client's documented instructions, including with regard to transfers of your Personal Data to a non-EEA country, unless not required to do so by laws and regulations applicable in EEA 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 countries prohibit such information on important grounds of public interest.

EEA & BCR

If a TP Company is not in a position to comply with a Client's reasonable instructions, it shall promptly inform both the Privacy Office and the Client, and Teleperformance will try to accommodate the Client's instructions taking into consideration local laws and regulations applicable in EEA 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 countries, the transfer of your 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 your 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), in which case Teleperformance shall certify to that Client that it has done so. Such return or destruction should be done within a 30-day timeframe after the termination of the contract between the Client and Teleperformance, which can be extended to 90 days (or more with the CPO's agreement), depending on the timeframe agreed in that contract.
When laws and regulations require storage by Teleperformance of your Personal Data transferred, it shall inform the Client and warrant that it will guarantee the confidentiality of your Personal Data, and will not actively process that Personal Data anymore.

1.2.3. Help Clients to handle your requests

Teleperformance shall assist Clients with handling any requests when you exercise your rights, including requests to access, correct or delete your 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 your requests for exercising your rights, including by providing any useful information in order to fulfil your requests.

EEA & BCR

When Teleperformance directly receives a request from you, it will promptly communicate it to the relevant Client, in which case the Client remains responsible for handling it, 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

EEA & BCR

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 your 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 countries to Process your 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.

EEA & BCR

If the Client 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 & data protection reason in accordance with laws and regulations applicable in EEA 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 your Personal Data

EEA & BCR

Transfers of your 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 TP Company based in the EEA transfers your Personal Data to one of the following:

- 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
- 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 your 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 a TP Company based in the EEA transfers your 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 your 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.

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

EEA & BCR

When an EEA TP Company transfers your 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 your 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., you have given your consent to the transfer; or the transfer is necessary for the performance of a contract between you and the Client or the implementation of pre-contractual measures taken in response to your 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 your Personal Data is not repetitive and concerns only a limited number of Data Subjects; the legitimate interests of the Client are not overridden by your 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 you of the transfer and the compelling legitimate interests.

2.3 Transfer from non-EEA countries to other countries

This describes the transfer of your Personal Data by a non-EEA TP Company to a Sub-processor or Third Party Data Processor based in another country. An example would be a transfer of your 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 your Personal Data from a non-EEA 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 your Personal Data or pertaining to security.

EEA & BCR

When your Personal Data transferred from the EEA to non-EEA Sub-processors or Third Party Data Processors are further transferred to other non-EEA Sub-processors or Third Party Data Processors, the EEA TP Company at the origin of the transfer shall ensure that such onward transfers comply with the rules set in Part 3, Section 0 above.

3 Information Security

3.1 Security and Confidentiality

TP Companies shall implement appropriate technical and organizational security measures to protect your 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 your rights and freedoms, by the nature of your 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 your 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 your 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.

EEA & BCR

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 cooperation with the relevant Chief Information Officer, the Global Chief Information Security Officer, the Local Privacy Lead, 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 you 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.

EEA & BCR

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 48 hours), as well as 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 Cooperation with DPAs

It is the duty of all TP Companies and their employees 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.

EEA & BCR

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

5 Cooperation 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 provide reasonable assistance.

6 Complaint handling

When a Client reports your complaint related to compliance with the requirements of Parts 1 and 3 of the Policy marked with "BCR" concerning the Processing of your 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 your complaint is handled in accordance with the procedure described below.

BCR

When you wish 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 your 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, you can lodge a complaint directly with Teleperformance by sending an email to privacy@teleperformance.com.

In both situations described above, the Privacy Office, or Local Privacy Leads, when appropriate, shall handle your complaint in accordance with the following procedure:

• Your identity shall be verified before assessing a complaint about the Policy. Additional forms of identification can reasonably be requested to verify your identity;
• Send you an acknowledgment of receipt and inform you about the procedure and timelines to respond;
• Based on the information contained in your complaint, assess whether it is justified, and investigate to understand the circumstances of the Processing subject to your complaint (e.g., extent of the infringement subject to your 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 two months from receipt of your complaint; and inform you of the result of the investigation and of the remediation measures implemented;
• When a substantive response to your complaint cannot be provided within one month because of the complexity and/or number of the complaints, notify you 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 you of the result of the investigation; and
• No matter whether or not your complaint is justified, inform you that you may escalate the complaint to the CPO if you are not satisfied by the response received to your complaint.

BCR

While Teleperformance encourages you to use the Client's dedicated complaint handling procedure (or Teleperformance's dedicated complaint handling procedure if the Client has factually disappeared, ceased to exist in law or has officially become insolvent without any successor entity), you 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 your 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 your identity you; or
• Your right is expressly restricted by laws and regulations applicable in EEA countries.

7 Your third-party beneficiary rights

Subject to Part 3, Section 8.1 of the Policy, when your Personal Data subject to laws and regulations applicable in EEA countries were transferred to non-EEA TP Companies or third parties on the basis of the Policy, you are entitled to directly seek a remedy against Teleperformance in respect of infringements of Part 1, Sections 3 (Scope) and 4 (Conflict between the Policy and local laws and regulations), as well as Part 3 of the Policy.

Subject to Part 3, Section 8.1 of the Policy, when your Personal Data subject to laws and regulations applicable in EEA countries were transferred to non-EEA TP Companies or third parties on the basis of the Policy, and you 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, you are entitled to seek a remedy in respect of infringements of Part 1, Sections 2 (Purpose limitation), 3 (Scope), and 4 (Conflict between the Policy and local laws and regulations), as well as Part 3 of the Policy.

BCR

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

You can choose to lodge your claim before:

• The courts with jurisdiction over the EEA Client or TP Company at the origin of the transfer;
• The courts with jurisdiction over the place where you have your habitual residence in the EEA; or
• The EEA DPA responsible for the EEA country in which you have your habitual residence, work, or where the alleged infringement took place.

8 Liability

8.1 Towards you

Subject to Part 3, Section 7, 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 TP Companies and to pay compensation for any material or non-material damages resulting from such infringement. In this case, you will have the same rights and remedies against Teleperformance SE as if an infringement had taken place in the EEA.

Subject to Part 3, Section 7, 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 TP Companies or non-EEA Third Party Data Processors, and to pay compensation for any material or non-material damages resulting from such infringement. In this case, you will have the same rights and remedies against Teleperformance SE as if the infringement had taken place in the EEA.

BCR

Such liability extends only to Data Subjects whose Personal Data subject to laws and regulations applicable in EEA countries were transferred to non-EEA TP Companies or non-EEA 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, you 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 TP Company nor a non-EEA 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.

8.2 Towards Clients

The Policy is 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 that 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 TP Companies; or
- The written contract signed with a non-EEA Third Party Data Processor, in accordance with Part 3, Section 1.2.4 of the Policy.

BCR

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 TP Company or non-EEA 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 Third Party Data Processor, in accordance with Part 3, Section 1.2.4 of the Policy.

9 Conflict between the Policy and local laws and regulations

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

Notwithstanding the requirements provided in Part 1, Section 4 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).

EEA & BCR

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 the matter to the EEA DPA applicable to the Client and the CNIL. 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 in order 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 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.

EEA & BCR

If Teleperformance receives any legally binding request for disclosure of your Personal Data Processed on behalf of a Client by a non-EEA 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 DPA applicable to the Client and the CNIL 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 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 DPA applicable to the Client and the CNIL, 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 DPAs.

In any case, transfers of your 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.

Annex 1 – Request and complaint handling procedure for Data Controller activities

This procedure implements and further defines the request and complaint handling mechanism set out in Part 2, Section 8 of the Policy.
This procedure provides minimum requirements, which all TP Companies Processing your Personal Data and being subject to privacy and data protection laws and regulations applicable in EEA countries shall follow, when they act as Data Controllers.

This procedure is subject to the Policy. In the event of discrepancies, the Policy takes precedence.

1. Steps for handling a your request or complaint

Step 1 – Receipt of request or complaint
When a TP Company receives your request or complaint, it shall be documented and communicated to the Privacy Office without undue delay and not later than 2 (two) days from the receipt.

If your request or complaint is sent directly to the Privacy Office, it shall be logged within the same timeframe from receipt.

Step 2 – Acknowledgement and allocation
The Privacy Office shall acknowledge receipt of your request or complaint within 1 (one) week and inform you that you will receive more information on your request or complaint within 30 (thirty) days of receipt.
Within 1 (one) week, the Privacy Office shall validate your request or complaint, and determine whether it will handle your request or complaint directly, or delegate it to a designated local contact point.
When the Privacy Office delegates your request or complaint to a designated local contact point, it shall provide additional instructions to such local contact point on how to handle your request or complaint to the extent necessary.

Step 3 – Request and complaint handling
The Privacy Office or, when appropriate, the local contact point, under supervision of the Privacy Office, will then handle your request or complaint.
Step 4 – Request or complaint completion
The Privacy Office or, when appropriate, the local contact point, under supervision of the Privacy Office, shall respond to your request or complaint within the timeframe set out in the section 'Resolution Timeframe'.

2. Responsibilities

Your identity shall be verified before granting your request to exercise your rights or, to the extent possible, before assessing your complaint about the Group Data Privacy Policy. Additional forms of identification can reasonably be requested to verify your identity.

Based on the information contained in your request or complaint, the Privacy Office in coordination with the local contact point, or, when appropriate, the local contact point in coordination with the Privacy Office, shall assess whether your request or complaint is justified, and investigate to understand the circumstances of the Processing subject to your request or complaint (e.g., extent of the infringement subject to a complaint).

When the investigation reveals that your request or complaint is justified, the Privacy Office or, when appropriate, the local contact point in coordination with the Privacy Office, shall you of the result of the investigation and of the remediation measures implemented.

When the investigation reveals that your request or complaint is not justified, the Privacy Office or, when appropriate, the local contact point in coordination with the Privacy Office, shall inform you of the result of the investigation.

Whether or not your request or complaint is justified, you shall be informed that you may escalate your request or complaint to the CPO if you are not satisfied by the response received to your request or complaint.

When your Personal Data is rectified, erased, or restricted pursuant to your request, and your Personal Data have been disclosed to recipients within Teleperformance or to third parties who are Data Controllers or Data Processors, each third party shall be informed of the rectification, erasure, or restriction unless this proves impossible or involves disproportionate effort. Teleperformance shall also inform you about the recipients to whom your Personal Data have been disclosed if you request it.

When you request a copy of your Personal Data and your request is made electronically, the information should be provided in an electronic format, unless otherwise requested by you.

All Personal Data that do not relate to you shall be redacted from any document provided to you. Other business data which is not Personal Data, or is not relevant regarding your request or complaint, may be redacted by the Privacy Office or local contact point.

3. Costs Associated with your Rights Request or Complaint about the Group Data Privacy Policy, and Refusing to Act on your Request or Complaint

Your request and complaint must be handled free of charge, unless the Privacy Office deems a request or complaint (or requests or complaints) from a particular Data Subject is (or are) manifestly unfounded, excessive or repetitive. If your request or complaint is manifestly unfounded, excessive, or repetitive, Teleperformance may:

• Charge a reasonable fee, taking into account the administrative costs of providing the information or communication, or taking the action requested; or
• Refuse to act on your request or complaint.
The Privacy Office shall demonstrate the manifestly unfounded, excessive or repetitive character of the request, requests, complaint or complaints when refusing to act.
Requests or complaints may also be rejected when:
• Processing does not involve Personal Data or data that can be used to identify a natural person directly or indirectly, and Teleperformance can demonstrate it is not in a position to identify a natural person; or
• The right of the Data Subject is expressly restricted by laws and regulations applicable in EEA countries.

4. Resolution Timeframe

The Privacy Office or, when appropriate, the local contact point in coordination with the Privacy Office, shall respond to your request or complaint in a timely fashion and, at the latest, within 1 (one) month of receiving your request or complaint.

Only the Privacy Office can extend by a further 2 (two) months the time to respond to your request to exercise rights or complaint about the Group Data Privacy Policy, for instance because of the complexity and/or number of the requests or complaints. If the Privacy Office extends the time to respond, the Privacy Office will immediately notify you and explain the reason for the extension.

Teleperformance

Transforming Passion into Excellence