BINDING CORPORATE RULES AS PROCESSOR

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivPol-01

Date	Version	Comments
17/08/2021	2.1	Division BCR-CONT / BCR-PROC

CONTENTS

1. INTRODUCTION

At Webhelp, we believe that protecting Personal Data is not only a matter of security or compliance with a particular legal framework, but is a matter of individual and organisational commitment. Disclosing and sharing Webhelp standards through Webhelp Privacy Policy (hereinafter, the "**Privacy Policy**") composed of Webhelp Binding Corporate Rules for Controllers (hereinafter the "**BCR-C**) and the present Binding Corporate Rules for Processors (hereinafter the "**BCR-P**") is of the utmost importance regarding the Data Subjects' legitimate expectations about how their Personal Data is Processed.

In the course of its activities, Webhelp processes both internal and Client Personal Data. In this respect, Webhelp protects the Personal Data it processes on behalf of its Clients by the implementation of appropriate technical, physical and administrative measures and controls crompised in the present BCR-P . Such controls shall ensure that the whole organisation is Processing Personal Data in a consistent manner, disregarding the nature and/or place of Processing.

This approach is particularly important due to the diversity of activities Webhelp covers on behalf of its Clients.

Webhelp BCR-P covers all Processing of Client Personal Data carried out by Webhelp Entities acting as Data Processor on behalf of Clients, acting as Data Controllers.

As a consequence of the above and taking into consideration the requirements introduced by the European Regulation 2016/679 adopted on 27 April 2016 (hereinafter, the "**EU Regulation"**) and standards, regulations and laws applicable in the field of data protection, where they do not contrevene with the EU Regulation Webhelp will Process Personal Data in accordance with the following principles:

- **Lawfulness** – Personal Data shall be collected and Processed with the Data Subject having given consent to the Processing or when Processing is legitimate or necessary in accordance with Applicable Data Protection Legislation;
- **Fairness** – Personal Data Processing shall take into account the specific circumstances and context in which such Personal Data is Processed;
- **Trans parency** – Information and communication relating to the Processing of Personal Data shall be easily accessible, easy to understand, clear and in plain and simple language;
- **Purpose limitation** – Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
- **Data minimisation** – Collected Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;
- **Accuracy** – Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without undue delay;
- **Storage limitation** – Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed or any other lawful retention;
- **Integrity and confidentiality** – Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical, physical and administrative measures.

Through this BCR-P Webhelp intends to share and specify the detail and the principles applicable to all Webhelp Entities and provide certain group-wide standards allowing the implementation of the BCR-P. Furthermore, Webhelp may make available specific, local or sectorial policies. Should there be a contradiction between this BCR-P and such specific, local or sectorial policies, the terms of the BCR-P shall prevail, unless the contradictory provisions of such specific, local or sectorial policies are more protective of the Data Subject rights and freedom..

As the this BCR-P aims at ensuring an adequate and consistent approach throughout the entire Webhelp organisation regarding Personal Data Processing, exceptions which could result from applicable legislations are not reflected in this this BCR-P. However, this BCR-P comprises a notification mechanism in section 13.3 where

national legislation prevents a Webhelp Entity from complying with the this BCR-P and where specific rules adding to the EU Regulation are provided by EU Member States. As a consequence, local legislation shall be considered as an enforceable exception to this BCR-P and will be recorded accordingly, following appropriate notification. As specified in section 13.3, where this national legislation imposes a higher level of protection for Personal Data, this national legislation will take precedence over the BCR-P.

2. SCOPE

2.1 Material scope

This BCR-P is applicable whenever a Webhelp Entity Processes Personal Data as Data Processor.

Due to the diverse range of activities Webhelp covers and the fact that Webhelp processes mainly Personal Data on behalf of its Clients, Webhelp may have to process various and constantly evolving categories of Personal Data, such as:

- Data relating to personal life (e.g. customer satisfaction monitoring, management of online social interactions);
- Economic and financial data (e.g. management of customer relation, fraud prevention and detection, invoicing, reporting and analytics,
- Identification data (e.g. inbound and outbound call management, management of opt-out operations, dialling & interaction routing, listening and recording interactions) ;
- Technical data (e.g. dialling & interaction routing, analytics for inbound and outbound operations, speech analytics solution); or

The material scope is more precisely detailed in **Appendix 11-B** which provides a detailed table on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-P.

Notwithstanding the above, this BCR-P applies to the Processing of Personal Data by Webhelp acting as Data Processor, irrespective of the category and nature of such Personal Data.

Webhelp is also the Data Controller of the Personal Data of its employees as their employer. When processing Personal Data of Webhelp employees, Webhelp will comply with the BCR-C and will process Personal Data as described in the Webhelp Employee Privacy Policy.

2.2 Geographical scope

Webhelp wants to ensure a consistent approach within the entire Webhelp Group where Personal Data are being Processed. Consequently, all Webhelp Entities, whatever their location or legal jurisdiction, are subject to this BCR-P. As a principle, no transfer of Personal Data shall be carried out by any Webhelp Entity unless and until it is bound by this BCR-P to a Webhelp entity not bound by this BCR-P. Any such transfer cannot be carried out unless such Webhelp entity has provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing and obligations attached to such Processing will meet the requirements of this BCR-P and ensure the protection of the rights of the Data Subjects. The Webhelp Entity bound by the BCR-P and the Webhelp entity not bound will enter into a written agreement to guarantee this.

3. BINDING NATURE

3.1 Upon employees of Webhelp

As protecting Personal Data is a matter of individual and organisational commitment, each employee must comply with the requirements specified under this BCR-P.

As such, the BCR-P falls within the set of policies Webhelp employees are required to comply with as part of their employment contract. Failure to comply with the principles and rules of this BCR-P may lead to disciplinary action that could result in the termination of the employment and, in certain circumstances, to criminal charges.

3.2 Upon entities of the Webhelp Group

As a group, Webhelp wants to ensure that all entities belonging thereto are bound in the same or a similar manner to the principles and obligations specified under this BCR-P and will comply with the requirements specified herein.

For this reason, this BCR-P is binding upon all the entities of the Webhelp Group by signing the Intragroup Data Transfer Agreement comprising this BCR-P as an appendix. .

The list of Webhelp Entities bound by this BCR-P is set out in Appendix 1 to this BCR-P. Webhelp commits to keep this list up-to-date and available and to communicate it on request to the relevant parties as determined from time to time.

3.3 Towards Webhelp's Clients

When acting on behalf of its Client as a Data Processor, the Webhelp Group undertakes to comply with this BCR-P and to implement the requirements thereof vis-à-vis its Clients and the Clients' Data Subjects. Where Webhelp is Processing the Personal Data of Data Subjects of its Clients, Webhelp as well as each Webhelp employee involved in the Processing undertakes to ensure, in accordance with any Clients' instructions, the protection of the rights of such Data Subject and provide an adequate level of protection to the Personal Data it processes subject to the provision of Section 7 – Rights of Data Subjects.

Any Processing activity carried out by a Webhelp Entity on behalf of a Client shall be governed by a written contract or other binding legal act, and shall set out (all elements of article 28 GDPR and in particular the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Data Controller. .In addition, this contract or other relevant binding legal act shall set out the following provisions:

i. Webhelp shall keep the Personal Data confidential.
ii. Webhelp shall take appropriate technical, physical and organizational security measures to ensure an appropriate level of security to protect the Personal Data.
iii. Webhelp shall not permit Sub-Processor to Process Personal Data in connection with its obligation to the Client without the prior written authorization of this latter, and shall ensure this Sub-Processor undertakes to comply with the same obligations as provided in the binding act executed between Webhelp and the Client.
iv. Webhelp shall make available to the Client all information necessary to demonstrate its compliance and contribute to audits and inspections by the Client or other relevant authority.
v. Webhelp shall promptly inform the Client of any actual or suspected security breach involving Personal Data and support the Client in the notification to the relevant Supervisory Authority and communication to affected Data Subjects as the case may be.
vi. Webhelp shall provide all reasonable assistance to the Client to conduct data protection impact assessment.
vii. Webhelp shall provide all necessary support to the Client in regards to the handling of requests from Data Subjects relating to their rights
viii. Webhelp shall comply with the Client's instructions regarding the deletion or return of the personal data at the termination of the contract or other legal binding act.
ix. Webhelp shall immediately inform the Client if, in its opinion, an instruction infringes this BCR-P or Applicable Data Protection Legislation.

Such contract shall include this BCR-P so as to disclose and enforce Webhelp Binding Corporate Rules upon both parties; Clients are entitled to enforce any provision of this BCR-P against Webhelp - or any Webhelp Entity with delegated responsibility.

3.4 Towards Webhelp's Data Processors

Where Webhelp engages another Data Processor, be it another Webhelp Entity or a third-party provider, for carrying out specific Processing activities, such Data Processor shall provide sufficient guarantees to implement appropriate technical and organisational measures in a manner that the Processing will meet the requirements of this BCR-P, and if necessary the Service Agreement between Webhelp and a Data Controller.

Data Processor will process Personal Data only on Data Controller documented instructions. Any Processing activity undertaken by Webhelp's Data Processors shall be governed by a written contract or other binding legal act, and shall set out all elements of article 28 GDPR and in particular the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of Webhelp. The binding act executed with the Webhelp's Data Processor shall contain the elements listed in section 3.3 above.

4. PRINCIPLES FOR PROCESSING PERSONAL DATA

When acting on behalf of its Clients as a Data Processor, Webhelp shall comply with the principles defined hereunder. In any case, the Client shall be responsible for all Personal Data Processing, whatever the origin of the Personal Data, conducted in accordance with the Applicable Data Protection Legislation, and the Service Agreement between Webhelp and the Client.

4.1 Transparency and fairness

Where acting as Data Processor, Webhelp commits to (1) provide sufficient guarantees and to implement appropriate technical and organisational measures in a manner that the Processing will meet the requirements of this BCR-P (2) cooperate with the Data Controller, within a reasonable time and to the extent reasonably possible, and to assist the Client to comply with the Applicable Data Protection Legislation. As Data Controller, Webhelp's Client remains responsible for ensuring that the Processing it requests from Webhelp is actually compliant with the Applicable Data Protection Legislation.

Taking into account the nature of the processing and the information available, Webhelp, through the Data Processing Standard Appendix completion, shall assist the Client where the Client believes a data protection impact assessment is required based on the nature, scope, context and purposes of the processing. To the extent the Client requires additional assistance to carry out a data protection impact assessment, to reply to investigations and enquiries of the data protection authorities or to seek prior consultation of the Supervisory Authority, Webhelp will, taking into account the nature of Processing and the information available to Webhelp, provide assistance to the Client through the Data Controller Audit Program.

In addition, Webhelp Entities shall ensure that Personal Data of the Client stored on production systems will be processed by Webhelp in accordance with article 28.3 (g) of the EU Regulation, upon termination of the Services Agreement. Unless any Applicable Data Protection Legislation or any other Service Agreement requires storage of the Personal Data and subject to the Data Controller's written request, Personal Data stored on production systems shall be, at the choice of the Data Controller, deleted or returned, upon termination of the Services Agreement. Webhelp will, within the time frame agreed with the Data Controller, have to warrant and guarantee the confidentiality of the Personal Data transferred by the Client and that Webhelp will not actively process the Personal Data transferred anymore. Data Controller acknowledges that this deletion or restitution of Personal Data (i) shall be strictly limited to Personal Data provided by the Data Controller and stored by Webhelp, acting as a Processor, at the moment of the request and (ii) shall take into consideration backup storage requirements and security policies and standards.

Moreover, where a Webhelp Entity has reasons to believe that applicable legislation prevents this Webhelp Entity from fulfilling its obligations under this BCR-P or has substantial effect on the guarantees provided by the BCR-P, this Webhelp Entity will promptly inform the DPO, Webhelp SAS and the other relevant Local Privacy Leader as well as Clients as provided in Article 13.3 (except where prohibited by applicable local legislation or a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In such case, the Client is entitled to suspend the transfer or the Processing activities at hand and / or to terminate the contract.

4.2 Purpose limitation

Webhelp undertakes to abide by a general principle of purpose limitation according to which it will only process the Personal Data on behalf of its Client and in strict compliance with its documented instructions where acting as Data Processor. Webhelp shall immediately inform the Client if in its opinion an instruction infringes the Applicable Data Protection Legislation.

More particularly, Webhelp undertakes to process Personal Data on behalf of its Client:

- for the sole purposes expressed by such Client;
- under the conditions agreed between Webhelp and its Client under the Service Agreement; and
- for no longer than what is expressly prescribed by the Client of Webhelp.

In the event a Webhelp Entity would not be able to provide such compliance, it undertakes to promptly inform its Client, the DPO and the relevant Local Privacy Leader of its inability to comply. Such information from Webhelp to its Client shall be made without delay and as soon as Webhelp is aware that such compliance is not reachable. In such a case, the Client would then be entitled to suspend the transfer of Personal Data to Webhelp or the Processing activities at hand and / or to terminate the contract.

4.3 Data quality

Webhelp undertakes to help and assist the Client to comply with the Applicable Data Protection Legislation.

In particular, Webhelp will assist its Clients in enabling Data Subjects to exercise their rights by executing any necessary measures requested by its Clients in order to have the Personal Data updated, corrected or deleted or any other right the Data Subject may enforce.

In such event, Webhelp will inform each Webhelp entity to whom the Personal Data have been disclosed of any correction, deletion or anonymization of personal data.

On request by its Clients and when feasible, Webhelp will also implement measures in order to have the Personal Data deleted or anonymised from the moment the identifiable form of such data is no longer necessary.

4.4 Record of processing activities

When acting as a Processor, Webhelp shall maintain a record of all categories of Personal Data Processing activities carried out on behalf of a Data Controller, that should at least mention:

- The name and contact details of Webhelp and of the Data Controller(s) on behalf of which Webhelp is acting;
- The categories of Processing carried out;
- The potential transfers of Personal Data to a third country or an international organisation;
- A general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the Processing.

4.5 Security

Where acting as Data Processor, Webhelp commits to comply with all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing, meeting at least the requirements of the Applicable Data Protection Legislation, and in particular article 32 GDPR and any existing particular measures specified in the Service Agreement with the Client.

Webhelp shall notify the Client without undue delay after becoming aware of a Personal Data breach and shall comply with the applicable Personal Data Breach procedure adopted by Webhelp in cooperation with the Data Controller.

4.6 Rights of the Data Subjects

Webhelp undertakes to execute any necessary measures requested by the Client and communicate any useful information in order to help such Client comply with its duty to observe the rights of the Data Subjects as further detailed under Section 7 of this BCR-P.

Taking into account the nature of the processing and the information available to the Processor, Webhelp shall provide assistance and cooperation to the Client, insofar as this is possible and agreed with the Client, for the fulfilment of the Client's obligation to respond to requests. Webhelp shall follow the Procedure for Data Subjects' requests where Webhelp acts as Data Processor annexed to this BCR-P.

Where Webhelp receives a request from Data Subjects to exercise their rights, Webhelp shall inform the Client and the latter shall respond to the request. In accordance with Applicable Data Protection Legislation, Client is liable for handling such request. Webhelp shall only be responsible for following its Client's further Instructions regarding how to handle such request and to co-operate with the Client for handling these requests.

4.7 Sub-Processing and onward transfers

Webhelp Entities or third-party providers may Sub-process Personal Data in accordance with the provisions of the Service Agreement as agreed with the Client. The Sub-Processors shall provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Data Processing will meet the requirements of the Applicable Data Protection Legislation, this BCR-P, and any applicable Data Processing Agreement.

Webhelp will not use a Sub-Processor without having first a written authorization from the Controller. When given a general authorisation to use Sub-Processors, Webhelp will inform the Client of any intended changes concerning the addition or replacement of any Sub-Processor and shall give the Client the opportunity to object to such changes and to terminate the applicable order form(s) as described here after and in Webhelp Service Agreement and Data Processing Agreement. Provided that the terms of applicable Webhelp Service Agreement and Data Processing Agreement and/or order form(s) do not deprive the Data Controller of the right to object or terminate the services, the Data Controller may terminate the applicable order form(s) with respect to those Services which cannot be provided by Webhelp without the use of the objected-to new Sub-Processor by providing written notice to Webhelp.

Sub-Processor shall be bound by way of a contract or other legal act that requires such Sub-Processor to comply with terms and obligations at least as stringent and that offer at least the equivalent level of protection than those described in the Data Protection Legislation, in this BCR-P and in a Data Processing Agreement. The Client may reasonably require Webhelp to communicate the list of Sub-Processors authorised to Process Personal Data. The contract shall precise the purposes of the Processing, its nature, the categories of Personal Data Processed and the categories of Data Subjects.

In case of a legal obligation to disclose Personal Data with the competent authorities, the involved Webhelp Entity must notify Webhelp SAS and the DPO. Webhelp SAS commits to notify the relevant EEA Supervisory Authority and unless otherwise prohibited the Client about this disclosure without undue delay and to comply with the Data minimisation principle. Webhelp shall precise which Data Subjects are concerned by the disclosure, which authority is asking for this disclosure and on which legal basis it is based on. In any case, Webhelp Entities commit not to transfer Personal Data to public authorities in a massive and disproportionate way. In that same case, Webhelp commits to notify the Client about the disclosure. Any notification within Webhelp and planned notification to EEA Supervisory Authorities are subject to the mechanism and provisions of Article 13.3 below.

In addition, each Webhelp Entity shall ensure and verify that all of its Sub-Processors and, in particular any other Webhelp Entity involved in the Processing of Personal Data, have been duly approved by the Client, either by a general or specific written authorisation.

5. PROCESSING SENSITIVE DATA

Webhelp undertakes to comply with the provisions of Section 4 – Principles for processing personal data and acknowledges that Sensitive Personal Data requires the implementation of specific protection as such Personal Data could create significant risks in relation to fundamental rights and freedoms of Data Subjects.

Where Webhelp is required by its Client to Process Sensitive Personal Data, Webhelp may be required to implement additional technical, physical and administrative security measures and controls.

It will be Webhelp's Client responsibility to define what measures should be implemented in this respect and to ensure that the requirements of the Applicable Data Protection Legislation and, where applicable, of any other sectorial applicable framework adopted by EEA Supervisory Authorities, are met.

For the sake of clarity, where it Processes Sensitive Personal Data as Data Processor, Webhelp shall in no event be responsible for ensuring that the Processing relies on one of the legal bases defined in the above Section 4 – Principles for Processing Personal Data.

6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

In the course of their business, Webhelp Entities may process Personal Data on behalf of its (or their) Client(s). Such Webhelp Entities or Client(s) may be located outside the European Economic Area (hereinafter "**EEA**"), and thus entail Transfers of Personal Data. In such a case, this BCR-P applies to:

- Personal Data received from a Client acting as Data Controller and located within the EEA which is then processed by Webhelp Entities, acting as Data Processors on behalf of this Client; and

- transfers of Personal Data from a Webhelp Entity acting as Data Processor on behalf of a Client and located within the EEA to a Webhelp Entity outside of the EEA, acting as Data Processor.

Otherwise where Personal Data is transferred, Webhelp will implement specific guarantees in order to ensure that the Personal Data transferred benefit from an adequate level of protection as further detailed below:

- Transfers of Personal Data from a Webhelp Entity acting as Data Processor to an entity of Webhelp or to third parties located outside of the EEA acting as Data Processor will be supported by a written agreement including the applicable standard contractual clauses adopted by the competent EEA Supervisory Authority and/or the EU Commission provided that the Data Controller allowed Webhelp to proceed to such Transfer on its behalf including any onward transfer; or;

- Transfers of Personal Data from a Webhelp Entity acting as Data Processor to an entity of Webhelp or to third parties located outside of the EEA as Data Controller will be supported by a written agreement including the applicable standard contractual clauses adopted by the competent EEA Supervisory Authority and/or the EU Commission provided that the Data Controller allowed Webhelp to proceed to such Transfer on its behalf, including any onward transfer.

In any event, Webhelp acting as Data Processor commits not to transfer Personal Data to third parties which are not part of the Webhelp Group without ensuring first that an adequate level of protection in line with the one provided by the GDPR will be granted to the Personal Data transferred.

For the sake of clarity, where a Webhelp Entity acts as Data Processor, it will only proceed with the Transfer under documented instructions from the Data Controller, unless required to do so by Union or Member State law to which that Webhelp Entity is subject. In such a case, Webhelp shall inform the Data Controller of that legal requirement before Processing the Personal Data, unless that law prohibits such information on important grounds of public interest as recognized in Union law or in the law of the Member State to which the Data Controller is subject.

7. RIGHTS OF DATA SUBJECTS

Where a Webhelp Entity acts as a Data Processor on behalf of its Clients, Data Subjects have to exercise their rights regarding the Processing of their Personal Data against Webhelp's Clients.

However, where the request of Data Subjects concerns requirements imposed on Data Processors, Data Subjects shall at least be able to enforce the following rights directly against Webhelp:

- Duty to respect the instructions from the Data Controller regarding the Personal Data Processing including for Transfers of Personal Data to third countries (Articles 4.2 and 6);
- Duty to implement appropriate technical and organisational security measures and duty to notify any Personal Data Breach to the Data Controller (Article 4.5);
- Duty to comply with the conditions when engaging a Sub-Processor either within or outside the Webhelp Group (Article 4.7);
- Duty to cooperate with and assist the Data Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Article 4.7);
- Easy access to the BCR-P on Webhelp website (currently at www.webhelp.com);
- Right to complain through internal complaint mechanisms (Article 8);
- Duty to cooperate with the EEA Supervisory Authority (article 13.4);
- Liability, compensation and jurisdiction provisions (Article 9);
- National legislation preventing respect of the BCR-P (Article 4.1);
- Duty to ensure the enforceability of third-party beneficiary rights (Article 7).

In any case, Data Subjects are:

- Entitled to seek judicial remedies for any breach of the rights guaranteed under this BCR-P and/or Applicable Data Protection Legislation (Article 9);
- Entitled to obtain redress and where appropriate receive compensation for a damage (including material harm but also any distress) resulting from the violation of the BCR-P by any Webhelp Entity (Article 9);
- Entitled to lodge a complaint before the EEA Supervisory Authority or courts competent for the Client located in the EEA (Articles 7.1. and 7.2).

Without prejudice to further recourses of Webhelp, where the Data Processor and the Data Controller 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 Webhelp.

In the event where it can be evidenced that the Client has factually disappeared or no longer exists in law or has become insolvent and that no other entity has assumed the legal obligations to recover the Client's obligations, Data Subjects are hereby expressly entitled to exercise the following rights and to bring a claim directly against the Webhelp Entity acting as Data Processor and bound by a Service Agreement with the Client:

- Duty to comply with the enforceable elements of the BCR-P (Articles 3.1 and 3.2)
- Duty to ensure the enforceability of third-party beneficiary rights (Article 7);
- The endorsement by Webhelp SAS of liability for paying compensation and to remedy breaches of the BCR-P resulting from a non-compliance with the BCR-P of a Webhelp Entity outside the EEA resulting in a recoverable damage, as well as the liability for demonstrating the Webhelp Entity in question is not liable for the alleged violation of the BCR-P which has resulted in the damages claimed by the Data Subject (Article 7.2)
- Easy access to the BCR-P on Webhelp website (currently at www.webhelp.com);
- Right to complain through the internal complaint mechanism of the companies (Appendix 5 – Article 3.1);
- Cooperation duties with EEA Supervisory Authority (Article 13.4);
- Duty to cooperate with the Data Controller (Article 4.1);
- Duty to comply with the principles for processing Personal Data listed under Article 4;
- To make available and update the list of entities bound by the BCR (Appendix 1); and
- National legislation preventing respect of BCR-P (Article 13.3);

7.1 Where a Webhelp Entity within the EEA does not comply with the BCR-P

Where a Webhelp Entity within the EEA does not comply with the BCR-P, and where the above conditions are met, Webhelp acknowledges that the Webhelp Entity within the EEA responsible of the non-compliance, shall bear responsibility and shall take the necessary actions in order to remedy its acts.

Webhelp also acknowledges that the Data Subject shall be entitled to

- lodge a complaint with an EEA Supervisory Authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement; and/or;
- an effective judicial remedy where he or she claims that this BCR-P has been infringed by Webhelp as Data Processor. Webhelp acknowledges that such claim can be brought either before the EU Member State where the Webhelp Entity responsible of the non-compliance is established or before the court where the Data Subject has his or her habitual place of residence.

7.2 Where a Webhelp Entity outside of the EEA does not comply with the BCR-P

Where a Webhelp Entity outside of the EEA does not comply with the BCR-P, Webhelp SAS (1) endorses responsibility for any damages resulting from the non-compliance with the BCR-P, including payment of compensation when granted by the competent court and (2) agrees to take the necessary actions in order to remedy the acts of such other Webhelp Entity.

In such circumstances, Webhelp SAS also acknowledges that the Data Subject shall be entitled to:

- lodge a complaint with a data protection authority where he/she has his/her place of residence, place of work or where the Webhelp Entity with delegated responsibility is established; and/or;
- an effective judicial remedy where the Data Subject considers that the Processing of Personal Data relating to him or her carried out by any Webhelp entity acting as Data Processor infringes this BCR-P. Webhelp acknowledges that such claim can be brought either before the Member State where the Webhelp Entity responsible for the non-compliance is established or before the court where the Data Subject has his or her habitual place of residence.

Webhelp SAS will be responsible for demonstrating that such Webhelp Entity outside the EEA is not liable for any violation of the rules specified under this BCR-P and which has resulted in the Data Subject claiming damages. In the event Webhelp SAS can demonstrate that the other Webhelp Entity located outside the EEA was not responsible for the act, then it can discharge itself from any responsibility.

Where the Controller can demonstrate that it suffered damage and evidences that it is likely that the damage has occurred because of a breach of this BCR-P by a Webhelp Entity outside the EEA, Webhelp SAS will be responsible for demonstrating that the Webhelp Entity outside the EEA or the external Sub-Processor outside the EEA was not responsible for the BCR-P breach that gave rise to the damages at hand or that no such breach took place.

7.3 Data Subjects' Rights

Data Subjects are entitled to benefit from the following rights:

- Have access to the Personal Data relating to him/her and Processed by Webhelp;
- Request the rectification or deletion of any inaccurate or incomplete Personal Data relating to him/her, and of any Personal Data with respect to which the purpose of Processing is no longer legal or appropriate;
- Request that the Personal Data Processing relating to him/her be limited;
- Object to the Processing of their Personal Data by Webhelp where such Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller, for legitimate interests purposes, including profiling at any time, on grounds relating to their personal individual situation, unless the interets pursued by the Client, acting as a Data Controller, override the interests rights and freedoms of the Data Subjects;

- Object to the Processing of their Personal Data by Webhelp where such Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, for marketing purposes, inluding profiling; and
- Receive their Personal Data in a structured, commonly used, machine-readable format and interoperable when the Processing is carried out by automated means

Where Webhelp is acting as Data Processor and receives a request from Data Subjects to exercise their rights, Webhelp shall inform its Client and the latter shall respond to the request. Webhelp shall only be responsible for following its Client's further instructions regarding how to handle such request. Webhelp will execute any necessary measures asked by the Client to have the Personal Data updated, corrected, deleted or anonymised from the moment the identification form is not necessary anymore. Webhelp shall communicate these instructions to any Webhelp Entity to whom the Personal Data have been disclosed. Webhelp will also execute any appropriate technical and organizational measures, insofar as this is possible, following the Clients' instructions, for the fulfilment of its obligation to respond to the requests, including by communicating any useful information. Where the Client has disappeared, or has ceased to exist or has become insolvent, Webhelp shall then handle such request directly to the extent possible and in accordance with the procedure it has adopted.

7.4 Exercising Data Subjects' Rights

Data Subjects are entitled to enforce this BCR-P as third-party beneficiaries, and to exercise their rights with respect to the Processing of their Personal Data by Webhelp as Data Processor acting on behalf of the Client.. Webhelp shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner.

Data Subjects can make a request verbally or in writing. Webhelp will provide Data Subjects with accessible means to exercise their rights and, in particular:

1 - A single dedicated contact email to be used irrespective of the country a Data Subject is located in:

Privacy@Webhelp.com

Local emails can be used in order to take into account local specificities, such as language.

To reach out your local privacy contact, please refer to **Appendix 01 - List of Webhelp Entities bound by the BCR-P and local Privacy email contacts.**

2 - Single portal and webform to be used irrespective of the country a Data Subject is located in accessible via an hyperlink on www.webhelp.com

3 - Single dedicated postal address to be used irrespective of the country a Data Subject is located in:

Group Data Protection Officer
Legal and Compliance Department
161 rue de Courcelles
75017 – PARIS
FRANCE

The DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the Requests, shall (i) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (ii), if deemed necessary, obtain as much information as possible to enable the Request to be duly handled.

If a doubt about the identity of the individual making the request exists, mainly when using distance communication means, Webhelp may be required to ask for more information regarding the Data Subjects. Information collected shall be (i) limited to information that is necessary to confirm who the individual making a request is and (ii) shall not be collected when products or services provided by Webhelp or its Clients are not delivered under the real identity of the user. Proportionality shall always be assessed by the Client acting as Data Controller.

In any case, the response to a Data Subject must occur within 1 month at the latest after receiving the Request (except in certain and limited circumstances as detailed in Appendix 6).

Where the Data Subject is not satisfied with the initial response provided by Webhelp such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined. Data Subject shall provide to Webhelp a detailed explanation of the unsatisfactory provisions of the solution previously provided. Webhelp shall

take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

If a Data Subject Request or complaint is rejected by Webhelp or the answer does not satisfy the Data Subject or in any case , the Data Subject can contact the DPO and / or can directly lodge a complaint with a competent EEA Supervisory Authority and / or to seek judicial remedy.

Further details regarding this Article are available in the following appendix:

- **Appendix 6 - Procedure for Data Subjects' requests where Webhelp acts as Data Processor**

8. DATA SUBJECTS COMPLAINT HANDLING PROCEDURE

Where a Data Subject communicates a complaint directly to Webhelp but the Client has not ceased to exist, not disappeared or has not become insolvent at the time such request was received by Webhelp, then Webhelp commits to inform the Client about such request without delay and in accordance with the procedure defined under **Appendix 6 - Procedure for Data Subjects' requests where Webhelp acts as Data Processor**.

In such a case, Webhelp undertakes to communicate any relevant information it receives from the Data Subject to the Client and agrees to expressly indicate to the Client that it is the Client's responsibility to handle such complaint.

Webhelp is not responsible for handling complaints made by Data Subjects when acting as Data Processor. However, in the event the Client has factually disappeared, ceased to exist in law or become insolvent, then Webhelp undertakes to handle complaints from Data Subjects pursuant to the same procedure as specified under Section 8 of the Webhelp BCR-C.

9. EXTERNAL CLIENTS' COMPLAINTS

Where a Webhelp Entity acting as Data Processor is non-compliant with this BCR-P, Webhelp acknowledges that the Client has the right to enforce this BCR-P against the non-compliant Webhelp Entity. The Client shall indeed be entitled to judicial remedies and has the right to receive compensation from the Webhelp Entity at the origin of the breach, subject to the provisions of the Service Agreement.

10. DATA PROTECTION GOVERNANCE

Webhelp has defined a Data protection organisation and governance which is further defined under **Appendix 3.** This organisation is led by the DPO who relies on a network of Local Privacy Leaders and business privacy referents.

The roles and responsibilities of the network as well as its working governance are further defined under **Appendix 3.**

11. PRIVACY BY DESIGN / PRIVACY BY DEFAULT

Where acting as Data Processor, Webhelp shall follow any reasonable instructions from the Client to allow the latter to comply with its obligations attached to Privacy by design and Privacy by default.

12. TRANSPARENCY AND COOPERATION

13.1 Communication of the BCR-P

Webhelp will openly communicate this BCR-P to the Data Subjects and make it easily accessible to any individual. Such communication shall allow any Data Subject to obtain a copy of this BCR-P with no undue delay and in an open format.

Webhelp will, in particular, allow the improvement of the privacy and security culture within its organisation by sharing this BCR-P through internal systems and means.

Where it is acting as Data Processor, Webhelp commits to share this BCR-P with its Clients and shall include this BCR-P in the Service Agreement in order to disclose and enforce Webhelp's BCR-P. In any case, where acting as Data Processor, as mentioned under Sections 3 and 4 of this BCR-P, Webhelp shall commit to comply with the BCR-P in relation to the Processing of its Clients' Personal Data.

13.2 Information to Data Subjects

Where it is acting as Data Processor, Webhelp is responsible for providing its Clients with relevant information enabling them to provide Data Subjects with relevant information required under Applicable Data Protection Legislation. However, Webhelp will not be responsible for providing mandatory information to Data Subjects as required under Applicable Data Protection Legislation as Webhelp's Clients are solely responsible in this respect.

13.3 Inconsistencies with local legislations

Where a Webhelp Entity has reasons to believe that its local legislation prevents it from fulfilling its obligations under this BCR-P , including any of the processing principles detailed in Article 1 above and has a substantial effect on the guarantees provided herein, then such Webhelp Entity must promptly inform (i) its Client(s), (ii) Webhelp SAS, (iii) the EU Webhelp Entity with delegated data protection responsibilities and (iv) the DPO or the relevant Local Privacy Leader / other privacy function.

Where Webhelp is acting as Data Processor, it also undertakes to promptly notify the data protection authority competent for its Client in such a case.

Where the relevant Webhelp body has been informed according to the above-mentioned notification mechanism, Webhelp SAS will notify the competent EEA Supervisory Authority. In such as case, Webhelp SAS commits to notify the relevant competent EEA Supervisory Authority about this legal requirement without undue delay and, , in the event such legal requirements mandates the disclosure of Personal Data by the Webhelp Entity at hand, to disclose only the necessary Personal Data in accordance with the relevant local legislation. Webhelp shall specify which Data Subjects may be concerned by this legal requirement or disclosure, which authority is asking for this disclosure and on which legal basis it is based on. In any case, Webhelp Entities commit not to transfer Personal Data to public authorities in a massive, indiscriminate and disproportionate way.

If a Webhelp Entity is legally prohibited from carrying out such notification, it should use its best efforts to waive this prohibition in accordance with the applicable local legislation. Webhelp SAS and this Webhelp Entity shall use their best efforts to circumvent prohibition to notify the Client and the relevant EEA Supervisory Authorities due to a local legislation mandating on a Webhelp Entity. To demonstrate its best effort to waive the prohibition, Webhelp shall document the action taken to this end and make it available to the relevant EEA Supervisory Authority. Where it is not possible to circumvent such prohibition, Webhelp SAS must provide annual general information regarding the numbers of disclosure of Personal Data to the relevant authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In addition, where a Webhelp Entity is subject to EU Member States national legislation adding some requirements or modalities which may have an impact on Processing carried out by Webhelp under this BCR-P, this Webhelp Entity shall promptly inform Webhelp SAS and document the complementary requirements applicable under this

national legislation. Where this national legislation imposes a higher level of protection for Personal Data, this national legislation will take precedence over the BCR-P.

Where a Webhelp Entity is subject to a non-EEA national legislation, which may have an impact on the processing of Personal Data under this BCR-P prior to the Transfer of Personal Data, an assessment of the laws and practices in the third country of destination which comprises notably: the specific circumstances of the transfer, the laws and practices of the third country of destination relevant in light of the specific circumstances of the transfer, and any relevant contractual, technical or organisational safeguards put in place, must be conducted in order to warrant that an adequate level of protection in line with the one provided by the GDPR will be granted to the Personal Data transferred

Where a Webhelp Entity located outside of the EEA has reasons to believe that it is or has become subject to laws or practices not in line with the above-mentioned assessment, it must promptly notify the Client or the EU Webhelp Entity, acting as Data Processor on behalf of that Client, which shall forward the notification to the Client. Following the notification, the Client and/or the EU Webhelp Entity acting as Data Processor must promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted to address the situation. If no appropriate safeguards for such Transfer can be ensured, the Transfer shall be suspended. In that event, the Client and/or the EU Webhelp Entity shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these BCR-P. If the contract involves more than two parties, the Client and/or the EU Webhelp Entity may exercise this right to termination only with respect to the relevant Webhelp Entity not able to grant an adequate level of protection to Personal Data, unless the parties have agreed otherwise.

13.4 Duty to cooperate

In any event, the Entities of the Webhelp Group agree to cooperate with EEA Supervisory Authorities, including by enabling such authorities to perform audits thereof, to take into account the advice, and to abide by decision of the competent EEA Supervisory Authority that may be provided in relation to this BCR-P.

Where acting as Data Processor, Webhelp commits to cooperate within a reasonable timeframe and to the extent reasonably possible with its Clients and to assist them to comply with the Applicable Data Protection Legislation. Webhelp shall also ensure that any Sub-Processor it uses to Process Personal Data is bound to comply with the same duty to cooperate and assist Webhelp and, as necessary, the Data Controller.

Webhelp and, where applicable, Webhelp's representative shall make available, upon request, the records of processing activities to the EEA Supervisory Authority only.

13. CHANGE TO THE BCR-P

Webhelp DPO will ensure that it keeps up to date a list of entities bound by the BCR-P. Where any new entity of Webhelp is effectively bound by the BCR-P (as specified in Article **Error! Reference source not found.**), Webhelp DPO shall update the list and shall inform without undue delay all Webhelp Entities and to relevant EEA Supervisory Authorities via the competent EEA Supervisory Authority. Data Subjects including Webhelp Employees and Clients will also be informed of such changes and such updated information will be made available to Data Subejcts together with the BCR-P and via the same means..

At least once a year, or when deemed necessary by the DPO, Webhelp will report such changes to the competent EEA Supervisory Authorities. The notification of such changes to EEA Supervisory Authorities will be carried out at least once a year via the competent EEA Supervisory Authority with a brief explanation of the reasons justifying the update.

To the same extent where an amendment has substantial impact on the BCR-P or on the level of protection of the rights granted by this BCR-P, Webhelp undertakes to promptly inform Webhelp Entities and EEA Supervisory Authorities.

o o

o

14. APPENDICES

Appendix 01	List of Webhelp Entities bound by the BCR-P and local Privacy email contacts
Appendix 02	Definitions for BCRs and Procedures
Appendix 03	Not Provided
Appendix 04	Not Provided
Appendix 05	Not Applicable to BCRs-P
Appendix 06	Procedure for Data Subjects' requests where Webhelp acts as Data Processor
Appendix 07	Not Provided
Appendix 08	Not Provided
Appendix 09	Not Provided
Appendix 10	Not Provided
Appendix 11-A	Not applicable to BCRs-P
Appendix 11-B	BCR-P List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)

Appendix 01 List of Webhelp Entities bound by the BCR-P and local Privacy email contacts

#	Webhelp Entity	Country	Privacy Email contact
1.	Webhelp Algerie	Algeria	privacy@dz.webhelp.com
2.	Webhelp Australia Pty Ltd	Australia	privacy@my.webhelp.com
3.	Webhelp Austria GmbH	Austria	privacy@de.webhelp.com
4.	Webhelp Payment Services Benelux SA	Belgium	privacy@wps.webhelp.com
5.	Les services Webhelp Inc.	Canada	protecciondedatos@onelinkbpo.com
6.	Webhelp Business Consulting Co. Ltd.	China	privacy@my.webhelp.com
7.	SELLBYTEL Group GmbH, organizační složka GmbH	Czech Republic	privacy@de.webhelp.com
8.	Webhelp Enterprise Sales Solutions s.r.o	Czech Republic	privay@cz.webhelp.com
9.	Webhelp Denmark AS	Denmark	privacy@nordic.webhelp.com
10.	Webhelp OÜ	Estonia	privacy@nordic.webhelp.com
11.	Webhelp Finland Oy	Finland	privacy@nordic.webhelp.com
12.	Webhelp SAS	France	Privacy@fr.webhelp.com
13.	Webhelp Enterprise SAS		
14.	Webhelp Conseil		
15.	W Automobile Services		
16.	Webhelp France		
17.	Webhelp Caen		
18.	Webhelp Compiègne		
19.	Webhelp Fontenay		
20.	Webhelp Gray		
21.	Webhelp Montceau		
22.	Webhelp Saint-Avold		
23.	Webhelp Vitré		
24.	Webhelp University France		
25.	Webhelp Prestations		
26.	Webhelp WTG		
27.	Webhelp WCS		

#	Webhelp Entity	Country	Privacy Email contact
28.	Marnix French ParentCO SAS	France	privacy@webhelp.com
29.	Marnix French TOPCO SAS		
30.	WowBidCo		
31.	WowMidCo		
32.	Marnix SAS		
33.	WowHoldCo		
34.	DMH3	France (Webhelp Medica activities)	privacy@directmedica.com
35.	Patientys		
36.	MED-TO-MED		
37.	Webhelp Medica		
38.	MSTV	France	privacy@fr.webhelp.com
39.	Netino	France	privacy@netino.webhelp.com
40.	Solvencia	France (WPS/WKS/Solvencia Services)	privacy@wps.webhelp.com
41.	Webhelp O2C Holding		
42.	Webhelp KYC Services		
43.	Webhelp Payment Services France		
44.	WPS Technology		
45.	Webhelp Payment Services Deutschland	Germany (WPS/WKS/Solvencia Services)	privacy@wps.webhelp.com
46.	Webhelp Holding Germany	Germany	privacy@de.webhelp.com
47.	Webhelp Deutschland		
48.	INVIRES GmbH		
49.	RIGHTHEAD GmbH		
50.	IQ-to-Link		
51.	Webhelp Hellas Business Enterprise Sales	Greece	privacy@gr.webhelp.com
52.	Webhelp India Private Limited	India	privacy@uk.webhelp.com
53.	SELLBYTEL Marketing Services India Private Ltd		
54.	Webhelp Payment Services Italia	Italy WPS/WKS/Solvencia Services)	privacy@wps.webhelp.com
55.	Webhelp Payment Services France succursale Italie		

#	Webhelp Entity	Country	Privacy Email contact
56.	Webhelp Enterprise Sales Solutions Italy Srl	Italy	privacy@it.webhelp.com
57.	Webhelp Cote d'Ivoire	Ivory Coast	privacy@ci.webhelp.com
58.	Webhelp (succursale Côte d'Ivoire)		
59.	Webhelp Japan KK	Japan	privacy@my.webhelp.com
60.	Webhelp LLC (Jordan)	Jordan	privacy@jo.webhelp.com
61.	IQ-to-Link shpk	Kosovo	privacy@de.webhelp.com
62.	Webhelp Latvia SIA	Latvia	privacy@nordic.webhelp.com
63.	Webhelp SIA		
64.	Webhelp Madagascar	Madagascar	privacy@mg.webhelp.com
65.	Webhelp Malaysia Sdn Bhd	Malaysia	privacy@my.webhelp.com
66.	Webhelp Mexico	Mexico	protecciondedatos@onelinkbpo.com
67.	Webhelp Maroc	Morocco	privacy@ma.webhelp.com
68.	Webhelp SAS Succursale Maroc		
69.	Webhelp Services		
70.	Webhelp Contact Center		
71.	Webhelp Multimedia		
72.	Webhelp GRC		
73.	Webhelp Technopolis		
74.	Webhelp University Maroc		
75.	Webhelp Agadir		
76.	Webhelp Fès		
77.	Webhelp Meknès		
78.	Webhelp Marrakech		
79.	Webhelp Netherlands Holding	Netherlands	privacy@nl.webhelp.com
80.	Customer Contact Management Group		
81.	Webhelp Nederland BV		
82.	Webhelp Enterprise		
83.	Stacelet Holding		
84.	Telecats BV		
85.	Netino Netherlands	Netherlands	privacy@netino.webhelp.com
86.	Webhelp Norway	Norway	privacy@nordic.webhelp.com

#	Webhelp Entity	Country	Privacy Email contact
87.	SELLBYTEL Group Philippines, Inc.	Philippines	privacy@my.webhelp.com
88.	Webhelp Poland	Poland	privacy@de.webhelp.com
89.	Webhelp Holding Germany GmbH (Sp. z o.o.)		
90.	Webhelp Sun Portugal Holding	Portugal	privacy@pt.webhelp.com
91.	Webhelp Oeiras		
92.	Webhelp Lisbon		
93.	Webhelp SAS Succursale em Portugal		
94.	Webhelp Braga		
95.	Righthead -Empresa de Trabalho Temporario Lda		
96.	DMHP Direct Medica Portugal	Portugal	privacy@directmedica.com
97.	Espana, Sucursal em Portugal	Portugal	privacy@wps.webhelp.com
98.	SELLBYTEL Group Puerto Rico LLC	Puerto Rico	protecciondedatos@onelinkbpo.com
99.	Webhelp Romania SRL	Romania	privacy@ro.webhelp.com
100.	Pitech Plus SA		
101.	Webhelp Senegal	Senegal	privacy@sn.webhelp.com
102.	Webhelp Singapore Pte Ltd	Singapore	privacy@my.webhelp.com
103.	Webhelp South Africa Outsourcing Proprietary Limited	South-Africa	privacy@uk.webhelp.com
104.	Serco Global Services South Africa Proprietary Limited		
105.	SELLBYTEL South Africa		
106.	Webhelp Malaga SLU	Spain	privacy@nordic.webhelp.com
107.	Webhelp Spain Business Process Outsourcing S.L.	Spain	privacy@es.webhelp.com
108.	Webhelp Spain Holding SLU		
109.	Webhelp Payment Services Espana	Spain (WPS/WKS/Solvencia services	privacy@wps.webhelp.com
110.	Telenamic	Suriname	privacy@sr.webhelp.com
111.	Webhelp Sweden AB	Sweden	privacy@nordic.webhelp.com
112.	Webhelp IT Services AB		

#	Webhelp Entity	Country	Privacy Email contact
113.	Webhelp Schweiz	Switzerland	privacy@de.webhelp.com
114.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.	Turkey	privacy@tr.webhelp.com
115.	Bin Çağrı Hizmetleri A.Ş.		
116.	Teknofix		
117.	Telecom Service Centres Limited	United Kingdom	privacy@uk.webhelp.com
118.	Webhelp Management Service (UK)		
119.	Dalglen (No.823) Limited		
120.	Webhelp UK Trading		
121.	Webhelp UK Holdings Limited		
122.	Go Beyond Services Limited		
123.	Webhelp Payment Services UK	United-Kingdom (WPS/WKS/Solvencia services)	privacy@wps.webhelp.com

Appendix 02 Definitions for BCRs and Procedures

"**Applicable Data Protection Legislation**"	Means in the following order of prevalence (i) the European Regulation 2016/679 relating to the Processing of Personal Data as of its date of application ("**GDPR**"), (ii) EU Member States national laws and regulations relating the Processing of Personal Data and implementing GDPR and (iii) any regulation relating to the Processing of Personal Data applicable during the term of this Privacy Policy.
"**Binding Corporate Rule**"	Means Personal Data protection policies and procedures which are adhered to by Webhelp for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor in one or more third countries within the Webhelp group.
"**Client**"	Means any third party, contracting with Webhelp and acting as Data Controller, whose Personal Data is Processed by a Webhelp Entity acting as Data Processor accordingly with its documented instructions.
"**Data**" or "**Information**"	Means any kind of information which is individually accessible by electronic or other means such as, but not limited to, logs, Personal Data, documents or other materials.
"**Database**"	Means a collection of independent works, data, Information or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
"**Data Controller**" or "**Controller**"	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determine the purposes and means of the Processing of Personal Data.
"**Data Processor**" or "**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, who can be identified, directly or indirectly, by means reasonably likely to be used by any natural or legal person, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
"**Device**"	Means any Programmable object that can automatically perform a sequence of calculations or other sequence of operations on Data once programmed directly or indirectly for the task. Any electronic apparatus adapted for displaying in a readable format, Information. Devices include but are not limited to computers, smartphone, tablets, laptops, servers, Networks, telephony platforms etc.
"EEA Supervisory Authority"	Means an independent public data protection authority which is established in an EEA Member State.
"**Encryption**"	A process to obfuscate data by transforming Data into a form in which there is a low probability of assigning a meaning or making it readable except when used in conjunction with a confidential process or key to decode it. Such process could be, but are not limited to mathematical function or algorithmic process
"**Information Administrator**"	Means the natural person within Webhelp organisation, alone or jointly with others, processes or manipulates the Information in accordance with the Information Owner needs', the objectives', purposes' and rules'.
"**Information Owner**"	Means the natural person within Webhelp organisation which, alone or jointly with others, determines the needs, the objective, purposes and rules of a project including Information processing.

"Intragroup Data Transfer Agreement"	Means the intra-group agreement which comprises the BCR-C and the BCR-P as appendices that all Webhelp Entities are required to execute in order to be bound by the BCR-C and BCR-P
"**Information Systems**"	Means any Device used directly or indirectly by a User or another Device in order to process Information including, but not limited toc collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Data
"**Local Privacy Leader**"	Means the person being the main point of contact of the DPO and dealing with data protection matters within each Webhelp Entity.
"**Malicious Software**"	Means software that by its introduction, adversely affects the intended function of software/hardware. This could include but is not limited to virus, malware, trojans, ramsomware etc.
"**Networks**"	Means the physical or logical connectivity that allows two or more Devices to communicate.
"**Password**" or "**Passphrase**"	Means a string of characters or any other logical or physical means used in conjunction with a User Identity during an authentication process to prove identity of a User and/or grand access to certain Information.
"**Personal Data**"	Means any information relating to an identified or identifiable natural person, (a 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. Personal Data includes Sensitive Personal Data.
"**Personal Data Breach**"	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;
"**Privacy and Data Council**"	Means Webhelp internal board supporting the Webhelp Group Data Protection Officer
"**Processing**" or "**Processed**"	Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**Pseudonymisation**"	Means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person;
"**Risk**"	Means a scenario describing an event and its consequences, estimated in terms of severity and likelihood.
"**Risk management**"	Means the coordinated activities to direct and control an organization with regard to risk.
"**Security Incident**"	Means attempted or successful unauthorised access, use, disclosure, modification, or destruction of Information or interference with system operations in the Information System.
"**Sensitive Personal Data**"	Means special categories of Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms requiring such Personal Data to merit specific protection as the context of their Processing could create significant risks to the fundamental rights and freedoms – such as Personal Data that reveals racial or ethnic origin, political opinion, religious or philosophical beliefs, or trade union employees,

	and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sexual orientation.
"**Service Agreement**"	Means the agreement entered into between Webhelp and its Client pursuant to which Webhelp provides services to its Client.
"**Sub-Processor**"	Means the entity engaged by a Data Processor for carrying out specific proces7 April 2021sing activities on behalf of the Data Controller, bound by the same data protection obligations as set out in the contract or other legal act between the Data Controller and the Data Processor
"**Software**" or "**Application**"	Means any code, instruction, programs routines that allows directly or remotely the manipulation of Data through any means and includes API, command shells etc.
"**Transfer of Personal Data**"	Means the Processing, material transfer or distant access to Personal Data from entities established outside of the European Economic Area (EEA).
"**User**"	Means all Webhelp employees, third parties, third parties' employees, contractors, contractors' employees and other persons whose conduct and duties allows the access to Webhelp Information Systems.
"**Webhelp**" or "**Webhelp Group"**	For the BCR and the related Procedures Webhelp shall mean Webhelp SAS and all entities listed in the List of entities bound by the BCR ("**Webhelp Entity**")

Appendix 03 Not Provided

Appendix 04 Not Provided

Appendix 05 Not Applicable to BCRs-P

Appendix 6

Procedures for handling Data Subjects' requests where Webhelp acts as Data Processor

1. INTRODUCTION

The adoption of the Binding Corporate Rules (i.e., "Webhelp Privacy Policy") by the Webhelp group and the commitment from the Webhelp entities to comply therewith demonstrates Webhelp's commitment to providing a high level of protection to the Personal Data it processes. Webhelp is committed to conducting business in accordance with the Applicable Data Protection Legislation including the European Regulation 2016/679 relating to the processing of Personal Data as of its date of application, any regulation relating to the processing of Personal Data applicable during the term of the Privacy Policy. As a consequence, Webhelp has implemented the following procedure.
The capitalised terms used herein shall have the same meaning as specified under the Privacy Policy.

2. OBJECTIVES OF THE PROCEDURE

Data Subjects, including employees of Webhelp, are granted specific rights regarding the processing of their Personal Data as further defined under Section 7 of the Privacy Policy.
When acting as Data Processor, Webhelp shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner as defined hereunder, in order to comply with the Privacy Policy and Applicable Data Protection Legislation. However, this shall only apply where Webhelp actually processes the requested information.
This document describes how Webhelp shall handle a Data Subject's Request where Webhelp acts as Data Processor (stakeholders, steps and timeline). Conversely, the Requests received from Data Subjects whose Personal Data is processed by Webhelp on its own behalf only, as a Data Controller, shall be handled according to the procedure specifically defined under the Policies and **Procedure 05 - Procedures for handling Data Subjects' requests where Webhelp acts as Data Controller**
In most cases, a Request from an individual (e.g. a Client's employee, client end user) will fall within the following situation:

- The processing conditions are not compliant with the Applicable Data Protection Legislation (e.g., health data not used, stored and/or encrypted in accordance with the local healthcare applicable law);
- The individual would like to exercise his/her privacy rights according to the Applicable Data Protection Legislation such as:
    - Accessing the Personal Data relating to him/her and processed by Webhelp on behalf of the Client he/she entered into a relation with;
    - Obtaining rectification, deletion or suspension of any inaccurate or incomplete Personal Data relating to him/her, or which is no longer processed for a valid or appropriate purpose;
    - Objecting to the processing of his/her Personal Data at any time, unless such processing is required by applicable law, provided that the individual demonstrates that he/she has a legitimate ground to object as it pertains to his/her particular situation; and
    - Receiving his/her Personal Data in a structured, commonly used and machine-readable format.

Even if such individual does not have a direct into relationship with Webhelp, there may be cases where Webhelp receives a Request directly from the individual and/or is asked by the Client to handle the Request on its behalf. **Webhelp shall in any case refer to the engagement with the Client to check whether specific conditions apply as to the handling of the Request** (e.g., interdiction to communicate directly with the Data Subjects etc.).
As a consequence, the cost and technical impacts of the Request must be anticipated and addressed at the beginning of each engagement.

3. PROCEDURES

Webhelp, acting as a Processor, is not responsible for informing Data Subjects of their rights in relation to Personal Data. Unless otherwise determined by applicable laws and regulation, such obligations are the responsibility of the Data Controller. Notwithstanding the above, Webhelp is committed to provide sufficient guarantees by implementing appropriate technical and organisational measures in such a manner that processing of Personal Data on behalf of the Data Controller will meet applicable requirements and ensure the protection of the rights of the Data Subject. Therefore, the procedures below apply where Webhelp acts as Data Processor on behalf of a Data Controller.

Since, it cannot formally be excluded that a Data Subject would send his/her Request directly to Webhelp, two different cases have to be considered.

3.1. Request directly received by Webhelp

3.1.1. Internal communication

Any employee or workforce of Webhelp receiving a Request in relation to Personal Data that Webhelp processes as Data Processor (e.g., on behalf of its Clients) must **immediately be** communicated to the Local Privacy Leader or Business Privacy Referent. Business Privacy Referent shall immediately inform its Local Privacy Leader, and Local Privacy Leader shall notify the Group Data Protection Officer ("**DPO**") of such Request.

The privacy emails to contact Local Privacy Leaders and/or Business Privacy Referents are provided in **Appendix 01 – B of the BCRs.**

As a matter of efficiency, such Request can also be communicated to the DPO through the following email:

Privacy@webhelp.com

The latter will then allocate the Request to the relevant Local Privacy Leader no later than 1 working day after receipt thereof.
The information provided by the employee or workforce of Webhelp must at least specify the following information:

- Name of the local manager in charge of the Client account;
- Copy of the Request; and
- Name of the Client the Data Subject's relates to.

Business Privacy Referent shall immediately inform its Local Privacy Leader

3.1.2. Transfer of the Request to the Client

Once it receives such Request, the Local Privacy Leader, will draft a communication to the Client about the Request. Such communication must (1) be sent by the Local Privacy Leader to the Client, in cooperation with the local manager in charge of the relationship with the Client; and (2) no later than 2 working days after receiving the Request. The Local Privacy Leader will also inform the DPO that the Request has been transferred to the Client.

3.1.3. Webhelp assistance to the Client.

At the same time, the Local Privacy Leader shall assess and verify if Webhelp actually processes the Personal Data of the Data Subject addressing the Request.
No answer shall be provided without Client's instructions
Should the Client allow Webhelp to handle the Request on its behalf, the Local Privacy Leader shall determine with the Client whether the Client itself or Webhelp shall acknowledge receipt of the Request and inform the Data Subject of Webhelp's role in the processing of his/her Request.
Unless otherwise expressly instructed by the Client, Webhelp shall not enter into contact with the Data Subject during the entire procedure.

3.1. Request sent by the Data Controller to Webhelp

3.1.1. Internal communication

Any employee or workforce of Webhelp receiving a Request from a Client in relation to Personal Data that Webhelp processes as Data Processor (i.e. on behalf of its Clients) must **immediately be** communicated to the Local Privacy Leader or Business Privacy Referent. Business Privacy Referent shall immediately inform its Local Privacy Leader, and Local Privacy Leader shall the DPO of such Request.
Where a Client sends to Webhelp a Data Subject's Request regarding the processing of his/her Personal Data to handle, Webhelp shall acknowledge receipt thereof to the Client no later than 2 working days after receiving such Request.
No later than 5 working days after the reception of the Request, Webhelp must verify the extent to which it can address and handle the Request.

3.1.2. Request Assessment

Upon receipt of a Request, either directly from the Data Subject or from the Client, and subject to the provisions and steps described in this Procedure, the Local Privacy Leader, or any other individual or entity, internal or external,

appointed by the Local Privacy Leader for the purpose of managing the following duties shall ensure and verify that he/she has all information necessary from the Client and the Data Subject to address his/her Request, in particular:

- Does the provided information allow Webhelp to identify the Data Subject? (i.e. Name and first name of the Data Subject);
- Description of the context in which the Personal Data was collected (if possible)
- Is Webhelp authorised to handle the Request on behalf of the Client?
- What is the nature of the Request? (access, deletion, opposition, rectification, portability)
- Does the Client consider the Data Subject's Request reasonable?
- Is it technically possible to address the Data Subject's Request (given in particular the volume of data at stake)?
- Do Webhelp have enough information regarding the scope of the Request? (geographical and material scope, Approximate date the data was collected;)
- Does the Data Subject already have possession or easy access to the requested Personal Data?
- Does the Request include information which is not in a clear format for Data Subjects? If yes, make sure you explain the codes so that the information can be understood.
- Are third parties involved in the processing of Data Subjects' Personal Data within the scope of the Request?
- Would the handling of the Request imply that third parties' Personal Data would need to be communicated to the Data Subject? If yes, is it possible to only extract the Personal Data of the requestor, with reasonable efforts and without a risk for the third parties' Personal Data?

Noteworthy, the gathering of such information must be limited to what is currently available within Webhelp. No additional information will be collected.
Webhelp shall refrain as much as possible from communicating with the Data Subject even if required by the Client. Where such request is sent to Webhelp, Webhelp shall first discuss with the Client the real opportunity to have Webhelp entering directly into contact with the Data Subject. If Webhelp accepts direct contacts with the Data Subject, Webhelp must inform the Client that the latter retains the entire responsibility vis-à-vis the Data Subject for handling in due course such Request.

3.1.3. Answer type identification

The Local Privacy Leader shall make sure that it examines the information provided by the Client and by the Data Subject within 8 working days from the time it receives the Request to determine if:

- He/she has the appropriate information to handle the Request; and
- He/she considers that the Request is reasonable (as opposed to a Request with no proof of the Data Subject identity, an excessive demand resulting from repetitive Requests, Request of Personal Data already deleted according to the retention period, Requests on behalf of others, etc.).

Three cases are then possible. These are as follows:

a. Case 1

Where the information provided by the Data Subject **is not sufficient** to handle the Request, the Local Privacy Leader, or any other individual or entity, internal or external appointed by the Local Privacy Leader for the purpose of managing the following duties, shall send a request for additional information to the Client no later than 2 working days after receiving the Request.
Where the Request is too complex, and subject to compliance with any legal requirement, the timeline of the response may be extended up to **20 working days**, subject to documentation of the assessment of the complexity by the Local Privacy Leader.

b. Case 2

Where the Local Privacy Leader considers on initial assessment, that the Request may **not be reasonable**, he/she shall not immediately close the case. The Local Privacy Leader, or any other individual or entity, internal or external, appointed by the Local Privacy Leader for the purpose of managing the following duties, shall reply to the Client within 10 working days after receiving the Request, by asking the Client to provide additional information as to why the Data Subject intends to exercise its rights.
Upon receipt of additional information, where the Local Privacy Leader still considers that the Request addressed by the Data Subject is not reasonable, the Local Privacy Leader shall document why it considers the Request is not reasonable and shall ensure, after approval of the DPO in writing, to reply to the Client or Data Subject, if expressly instructed by the Client, no later than 15 working days after receiving the additional information.
The response shall include the reason for not taking an action and the possibility for the Data Subject to lodge a complaint with a data protection authority and seek a judicial remedy. The wording of such response shall be validated by the DPO and the Client.

Where the Local Privacy Leader considers that, based on the additional elements, the Request can be handled it shall ensure that it addresses the request within the above mentioned 15 working days and shall inform the DPO accordingly.

c. Case 3

Where information provided by the Client and/or the Data Subject is sufficient, the Local Privacy Leader shall make sure that it responds to the Request, pursuant to the instructions of the Client, within 15 working days from the receipt thereof and duly informs in writing the DPO about the timing and content of the response so provided.

3.1.4. Escalation process

In the case of a complaint received directly from a Data Subject as to how its Request has been addressed, whether during or after the response has been given, the Local Privacy Leader shall ensure that it shares with the Client and the DPO the matter, no later than 3 working days after receiving the Data Subject's complaint.
For each of the above steps, and where necessary to handle the case appropriately, the Local Privacy Leader shall be ready to cooperate with the DPO by providing the latter with any relevant information in relation to the matter and inform the Client of the handling of the procedure.
The Group Data Protection Officer's guidance shall be binding. However, the DPO shall not enter into contact directly with the Data Subject, unless expressly required by the Client and the Local Privacy Leader.

3.1.5. Refusal of a Request

Although Webhelp is committed to handling Data Subjects' Requests efficiently, under certain circumstances as defined below, Webhelp may be entitled not to accept the Client or Data Subject Request.
Webhelp can oppose the Client's or Data Subject's Request, where agreeing to the Request would imply that the following information would be shared:

- information covered by the legal privilege;
- information which Webhelp is legally forbidden to communicate; and/or
- information Webhelp is processing during the course of an ongoing investigation or pending litigation procedure.

Where there is a conflict of privacy, Personal Data may be redacted before it is shared with the Client or the Data Subject.
In addition, in case of a Request received from the Client regarding a Data Subject opposing the further processing of his/her Personal Data and/or asking for the deletion of his/her Personal Data, Webhelp may refuse to grant such Request where legal obligations prevent Webhelp from doing so or where Webhelp has an over-riding legitimate interest. This shall be assessed on a case by case basis and referred to the DPO for a final decision before the Client or the Data Subject is informed.

3.1.6. Communication with Data Subjects

If the Client requires Webhelp to handle the Request on its behalf, the following rules shall apply when Webhelp communicates with the Data Subject.
Under no circumstances and unless otherwise expressly instructed by the Client, shall Webhelp enter into contact with the Data Subject during the entire procedure. Even if required by the Client, Webhelp shall refrain as much as possible from communicating with the Data Subject.
When communicating with the Data Subject, Webhelp shall cooperate with the Data Subject and address any Request in a timely manner. All communication shall be provided using clear and plain language, in an intelligible, concise, easily accessible and understandable form.
The information to be provided to Data Subjects shall be accurate and limited to (i) what the Data Subject has requested and (ii) the list of information that may be provided by a Data Controller according to the Applicable Data Protection Legislation.
The Local Privacy Leader shall pay particular attention to the deadlines mentioned in this Procedure.
As a general rule, Webhelp shall not apply fees for reasonable Data Subject Requests. However, under certain circumstances, in particular where the handling of the Request would imply important efforts from Webhelp, reasonable fees, subject to a national maximum according to applicable laws, may apply provided that the Data Subject is informed about such fees in advance.

-

Questions regarding this procedure or knowledge of a violation or potential violation of this procedure must be reported directly to the Group Data Protection Officer.

Appendix 07 **Not Provided**

Appendix 08 **Not Provided**

Appendix 09 **Not Provided**

Appendix 10 **Not Provided**

Appendix 11-A **Not applicable to BCRs-P**

Appendix 11-B BCR-P List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)

Appendix 11-B – Material Scope BCR-P List of Purposes of Processing and related Categories of Personal Data and Data Subjects

In addition to the provisions of section 2.1 on the material scope of this BCR-P, the table below provides further details on the transfers performed under this BCR-P. This table details on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-P The table below provides details about the transfers of personal data carried out between Webhelp Entities listed in Appendix 1 under this BCR-P.
The countries to which the personal data may be transferred depend of the localization of Webhelp Entities involved in the processing activities and is provided in Appendix 1

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
Operation & Marketing	*Contact centers related activities*	**Contact Center Operations Management**	**1.Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2.Professional data** (e.g. ,job title role, employee internal identification number, line reporting manager) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Personal life data (of End-customer)** (e.g., Marital status, number of persons in the household, number and age of children in the household, occupation, living habits and lifestyle, field of activity) **5. Contract management data** (e.g., Transaction number, details of the purchase, subscription, description, and conditions of the good or service purchased, History of the interaction between the End Customer and the Data Controller) **6. Loyalty programs and Outbound activities data** (e.g., Data necessary for the management and cycle of loyalty programs, prospecting, research, surveys, product testing and promotion) **7. Economic and Financial data** (e.g., information necessary to manage end-customer request such as	**Webhelp's employees Controller/Client 's End customer / Prospects**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
			Information on payment, payment terms (discounts, rebates, etc.), bank details)	
		Opt-out operations (in the course of outbound activities)	**1.Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2.Technical and connection data** (e.g., IP Address ,Logins ,Device ID data) **3. Contract Management Data** (e.g., Information regarding the Customer's decision to unsubscribe, including via a third party "do not call list)	**Webhelp's employees** **Controller/Client's End customer / Prospects**
		End-Customer satisfaction control	**1.Identification data** (e.g. Identification by the means used to interact with the Contact Center (telephone number, fax number, e-mail address, internal processing code allowing identification of the End-Customer) **2.Professional data** (e.g., job title role, line reporting manager, office location) **3. Technical and connection data** (e.g., IP Address, Logins ,Device ID data) **4. Contract management data** (e.g., aggregated responses provided, results of evaluation)	**Webhelp's employees** **Controller/Client's End customer / Prospects**
		Fraud Prevention and detection	**1. Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2. Professional data** (e.g., job title role, line reporting manager, office location) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Interaction data** (e.g., information on end-customer request, response provided, transcription of conversation)	**Webhelp's employees** **Controller/Client's End customer / Prospects**
		Monitoring, listening & recording interactions	**1. Identification data** (e.g., Name, Last name, E-Mail ,Phone number, Address, Internal processing code allowing the identification of the End Customer) **2. Professional data** (e.g., job title role, line reporting manager, office location, employee internal identification number) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Personal life data** (of End-customer) (e.g., Marital status, number of persons in the household, number and age of children in the household, occupation, living habits and lifestyle, field of activity) **5. Contract management data** (e.g., Transaction number, details of the purchase, subscription, description and conditions of the good or service purchased, History of the interaction between the End Customer and the Data Controller) **6. Loyalty programs and Outbound activities data** (e.g., Data necessary for the management and cycle of loyalty programs, prospecting, research, surveys, product testing and promotion) **7. Economic and Financial data** (e.g., information	**Webhelp's employees** **Controller/Client's End customer / Prospects**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
			necessary to manage end-customer request such as Information on payment, payment terms (discounts, rebates, etc.), bank details) 8. **Interaction data** (e.g., information on end-customer request, response provided, transcription of conversation)	
		Business Intelligence, reporting and analysis	**1.Identification data** (e.g., name, last name **2.Professional data** (e.g., job title role, line reporting manager, office location) **3. Technical and connection data** (e.g., IP Address, Logins ,Device ID data) **4. Contract management data** (e.g., aggregated stats on compliance with KPI imposed by the client)	**Webhelp's employees** **Controller/Client's End customer / Prospects**
		Numbering & Routing / interactions technical management	**1. Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address, Internal processing code allowing the identification of the End Customer) **2. Professional data** (e.g., job title role, line reporting manager, office location, employee internal identification number) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data) **4. Contract management data** (e.g., Information regarding the Customer's decision to unsubscribe, including via a third party "do not call list)	**Webhelp's employees** **Controller/Client's End customer / Prospects**
		Modification of the agent's voice to shape its expressivity and improve communication	**1. Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address) **2. Professional data** (e.g., job title role, line reporting manager, office location, employee internal identification number) **3. Technical and connection data** (e.g., IP Address, Logins, Device ID data)	**Webhelp's employees**
	Netino activities	**Moderation and online social interactions**	**1.Identification data** (e.g, Name, Last name , picture of the end customer (if published on the tool), E-Mail , Phone number, pseudo) **2.Technical and connection data** (e.g., IP Address ,Logins, Device ID data) **3. Interaction data** (e.g., access to data published by the data subject on a platform)	**Webhelp's employees** **Controller/Client's End customer / Prospects**

Domain of processing activities		Purpose of processing	Categories of Personal Data	Categories of Data Subjects
	WPS/WKS related services	**Collection and Analysis of KYC Documents (on behalf of ordering clients)**	**1.Identification data** (e.g., Name, Last name) **2. KYC information** (e.g., go/no go, results of KYC investigations)	**Client/Controller's end customer / prospect**
		Client Applicants Background Checks / KYE (on behalf of ordering clients)	**1.Identification data** (e.g., Name, Last name) **2. KYC information** (e.g., go/no go, results of KYC investigations)	**Client/Controller's end customer / prospect**