

Webhelp

BINDING

CORPORATE RULES

AS CONTROLLER

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

Date	Version	Comments
17/08/2021	0.2	Division BCR-CONT / BCR-PROC

CONTENTS		
1.	INTRODUCTION	3
2.	SCOPE	5
	2.1 Material scope	5
	2.2 Geographical scope	5
3.	BINDING NATURE	6
	3.1 Upon employees of Webhelp	6
	3.2 Upon entities of the Webhelp Group	6
	3.3 Towards Webhelp's Data Processors	6
4.	PRINCIPLES FOR PROCESSING PERSONAL DATA	7
	4.1 Defining a legal basis for Processing	7
	4.2 Defining a purpose	7
	4.3 Minimising Personal Data collection	7
	4.4 Holding a record	7
	4.5 Accuracy of the Personal Data	8
	4.6 Defining a data retention period	8
	4.7 Implementing security measures	8
	4.8 Data Protection Impact Assessment	8
	4.9 Transfers outside the Webhelp Group	9
	4.10 Implementing Personal Data Breach notification measures	9
5.	PROCESSING SENSITIVE DATA	11
6.	TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES	12
7.	RIGHTS OF DATA SUBJECT	13
	7.1 Where a Webhelp Entity within the EEA does not comply with the BCR-C	13
	7.2 Where a Webhelp Entity outside of the EEA does not comply with the BCR-C	13
	7.3 Data Subjects Rights	14
	7.4 Exercising Data Subjects' Rights	14
8.	DATA SUBJECTS COMPLAINT HANDLING PROCEDURE	16
9.	PRIVACY BY DESIGN / PRIVACY BY DEFAULT	17
10.	TRANSPARENCY AND COOPERATION	18
	12.1 Communication of the BCR-C	18
	12.2 Information to Data Subjects	18
	12.3 Inconsistencies with local legislations	18
	12.4 Duty to cooperate	19
11.	CHANGE TO THE BCR-C	20
12.	APPENDICES	1
	Appendix 01 - A List of Webhelp Entities bound by the BCR-C and local privacy email contacts	1
	Appendix 02 Definitions for BCR and Procedures	1
	Appendix 03 Not Provided	1
	Appendix 04 Not Provided	1
	Appendix 05 Procedure for Data Subjects' requests where Webhelp acts as Data Controller	2
	Appendix 11-A BCR-C material scope: List of Purposes of Processing and related Categories of Personal Data and Data Subjects	6

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 Processors (hereinafter the “**BCR-P**”) and the present Binding Corporate Rules for Controllers (hereinafter the “**BCR-C**”) 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 its own behalf by the implementation of appropriate technical, physical and administrative measures and controls, comprised in the present BCR-C . 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-C covers intragroup Processing of Personal Data between Webhelp Entities bound by the BCR-C, whenever one Webhelp Entity is acting as Data Controller or as Data Processor on behalf of another Webhelp Entities acting as Data Controller.

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 contravene 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;
- **Transparency** – 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-C 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-C. Furthermore, Webhelp may make available specific, local or sectorial policies. Should there be a contradiction between this BCR-C and such specific, local or sectorial policies, the terms of the BCR-C 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 BCR-C 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 BCR-C. However, this BCR-C comprises a notification mechanism in section 12.3 where national legislation prevents a Webhelp Entity from complying with the BCR-C 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-Cand will be recorded accordingly, following appropriate notification. As specified in section 12.3, where this national legislation imposes a higher level of protection for Personal Data, this national legislation will take precedence over the BCR-C.

2. SCOPE

2.1 Material scope

This BCR-C is applicable whenever a Webhelp Entity Processes Personal Data as Data Controller and as a Data Processor for Processing carried out within the Webhelp Group, on behalf of a Webhelp Entity acting as Data Controller.

Due to the diverse range of activities Webhelp covers, Webhelp may have to process various and constantly evolving categories of Personal Data, such as:

Data relating to personal life (e.g. recruitment management, camera recording system, client and prospect lead management) ;

- Economic and financial data (e.g. payroll management, client and prospect lead management,) ;
- Identification data (e.g. suppliers management, non-commercial communication, survey and form, client and prospect lead management) ;
- Technical data (e.g. IT and telephony management, badge management, employee record management) ; or
- Transactional data (e.g. corporate and legal entities management).

The material scope is more precisely detailed in **Appendix 11-A** 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-C.

Notwithstanding the above, this BCR-C applies to the Processing of Personal Data by Webhelp acting as Data Controller or as Data Processor on behalf of another Webhelp Entities acting as Data Controller, 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 this 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-C. 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-C to a Webhelp entity not bound by this BCR-C. Any such transfer cannot be carried out unless this 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-C and ensure the protection of the rights of the Data Subjects. The Webhelp Entity bound by the BCR-C and the Webhelp entity not bound will enter into a written agreement to guarantee this.

3. BINDING NATURE

3.1 Upon employees of Webhelp

Each Webhelp **employee**, as a Data Subject, shall benefit from the provisions of this BCR-C. As protecting Personal Data is a matter of individual and organisational commitment, each employee must also comply with the requirements specified under this BCR-C.

As such, the BCR-C 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-C 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-C and will comply with the requirements specified herein.

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

The list of Webhelp Entities bound by this BCR-C is set out in Appendix 1 to this BCR-C. 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 Data Processors

Where Webhelp engages a Data Processor, be it a 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-C.

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 listed below 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.

In addition, this contract or other binding legal act with a Data Processor shall set out the following provisions:

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

4. PRINCIPLES FOR PROCESSING PERSONAL DATA

The Applicable Data Protection Legislation defines a set of principles to be observed when Processing Personal Data. Webhelp undertakes to comply with these principles acting as Data Controller or Data Processor on behalf of a Webhelp Entity acting as Data Controller.

4.1 Defining a legal basis for Processing

When Personal Data is being Processed, it is required that such Processing relies upon an appropriate legal basis among the one provided in article 6 GDPR, such legal basis being the foundation that allows for lawful Processing.

In this respect, Webhelp undertakes to lawfully Process Personal Data only where it has a valid legal basis to do so pursuant to the requirements of the Applicable Data Protection Legislation.

For instance, the processing of Webhelp Employees' Personal Data is necessary to manage leave requests (e.g. holidays). Thus, the legal basis for such processing operation is the necessity to execute the employment contract Webhelp and its Employees have entered into.

4.2 Defining a purpose

Unless specifically authorised by Applicable Data Protection Legislation, Webhelp shall ensure that it has ascertained a lawful, fair, explicit and legitimate purpose prior to any collection or Processing of Personal Data.

Webhelp undertakes to ensure that the purposes it defines do not breach the Applicable Data Protection Legislation and appear to be legitimate while ensuring Personal Data is not further Processed in a manner that is incompatible with those purposes.

For instance, planning the necessary work force to deliver its services and consequently managing Webhelp Employees' schedules is one of the purposes defined for the collection of Employees' personal data regarding their request for leave.

4.3 Minimising Personal Data collection

Webhelp commits to collect and process Personal Data which is strictly adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

Personal Data shall not be collected widely in the perspective of a further undefined purpose.

For instance, Personal Data collected for managing request for leave is limited to the nature of the leave (e.g. holidays, maternity leave etc.) and other relevant information (e.g. duration of the leave), but it does not include any Personal Data which is not strictly necessary (such as with whom the Employee is going on holidays, the destination of the Employee or any health data for sick leaves).

4.4 Holding a record

When acting as a Data Controller, Webhelp shall maintain a record of all categories of Personal Data Processing activities under its responsibility that should at least mention:

- The name and contact details of Webhelp, the potential joint controller and the Data Protection Officer;
- The purposes of the Processing;
- The description of the categories of Data Subjects and of Personal Data;
- The categories of recipients of the Personal Data;
- The potential transfers of Personal Data to a third country or an international organisation;
- The Data storage duration;
- A general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the Processing.

For instance, the processing operation of managing Employees' requests for leave is included in the record of processing activities related to employee administrative management which contains the above listed information.

4.5 Accuracy of the Personal Data

Webhelp shall implement adequate measures and controls to ensure that the Personal Data it collects and processes remains accurate and, where necessary, kept up to date. To this end, Webhelp undertakes to implement any required actions to take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is Processed, is erased or rectified.

For instance, Employees have a duty to inform their HR department of any update in their personal situation (e.g. address modification). Webhelp will then ensure the Personal Data will be updated accordingly in the Employees' record.

4.6 Defining a data retention period

Webhelp will not keep the Personal Data for a longer period than is strictly necessary having regard to the purpose for which such Personal Data is collected. In this respect, Webhelp commits to determine a data retention period before implementing each Processing.

To ensure compliance with this requirement, Webhelp shall implement a data retention procedure and specify guidelines to be applied with respect to a given Processing activity.

For instance, Personal Data collected for managing leave request are kept as long as necessary to manage the schedules, perform action relating to payroll (e.g. unpaid leave) and to comply with applicable local statute of limitation and accounting obligations.

4.7 Implementing security measures

Webhelp has implemented appropriate technical, physical and administrative measures and controls to ensure that Personal Data is not unlawfully accessed and/or Processed. Such technical, physical and administrative measures shall ensure a level of security appropriate to the risk, including, but not limited to, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Webhelp and any Data Processor. In addition, Webhelp ensures that its subcontractors / Processors comply with the technical and organisational security measures implemented at Webhelp in entering into written agreements with them comprising the requirements set out in article 28.3 GDPR.

For instance, the Webhelp Group elaborated and implemented an Information Security Policy (Appendix 10 to this BCR-C). Locally, Webhelp Entities may have also implemented more specific security policies. When entering into an agreement with subcontractors / Processors, Webhelp reserves itself the right to assess the level of security provided by the contracting party to the Processing of Personal Data.

4.8 Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) is a risk-based process introduced by the General Data Protection Regulation that enables the Data Controller to describe the Personal Data Processing, to prove its necessity and proportionality and to help manage the risks to the rights and freedoms of natural persons resulting from the Processing of Personal Data by assessing them and determining the measures to address them. Webhelp is committed to conduct DPIAs in accordance with **Appendix 09 Procedure for Data Protection Impact Assessment**.

Where a type of Processing, involving in particular the use of new technologies, is likely to result in a high Risk to the rights and freedoms of Data Subjects, Webhelp shall, taking into account the nature, scope, context and purposes of the processing and prior to the processing, carry out a DPIA. This requirement shall also apply to existing processing operations where a modification of the processing operation is expected and where such modification may result in a high Risk to the rights and freedoms of Data Subjects.

The processing would require a Data Protection Impact Assessment if two or more of the following is correct:

- The Data processing includes systematic evaluation or scoring of personal aspects relating to natural persons, including profiling and predicting;
- The Data processing is based on automated processing that significantly affects the natural person;
- The Data processing is done on sensitive Data or on Data of highly personal nature;
- The Data is processed on a large scale;
- The processing combines or matches two or more Data processing operations;
- The Data processing includes a systematic monitoring of a publicly accessible area;
- The processing is made on vulnerable persons' or kids' Data;
- The Data processing includes innovative use or application or technological or organisational solutions;
- The Data processing is made for the purposes than those for which the Data were collected;

- The Data processing prevents the Data subjects from exercising their rights or using a service or contract.

In addition, Webhelp shall carry out a DPIA for processing operations that require a DPIA pursuant to a decision of the relevant EEA Supervisory Authority's list of data processing operations that require a DPIA.

Where a DPIA indicates that the processing would result in a high Risk in the absence of measures taken by the controller to mitigate the risk and where a DPIA reveals high residual Risks, Webhelp will seek prior consultation of the EEA Supervisory Authority before carrying out this Processing.

For instance, managing Employees' leave request is not a processing considered to present a high risks to the rights and freedoms of Data Subjects. Although, whenever Webhelp identifies a processing meeting two or more of the above-listed criteria, a DPIA is conducted under the supervision of the DPO in accordance with the procedure further described in Appendix 9.

4.9 Transfers outside the Webhelp Group

Webhelp undertakes not to transfer any Personal Data to Data Controllers and/or Data Processors which are not part of the Webhelp Group unless such Data Controllers and/or Data Processors provide sufficient guarantees and have implemented appropriate technical and organisational measures, such as the ones provided in the BCR-P, being part of Webhelp Privacy Policy, in such a manner that the Processing will meet the requirements of this BCR-C.

In this respect, Webhelp has implemented appropriate technical, physical and administrative measures to ensure and control that Personal Data is not unlawfully accessed and/or Processed.

Any Webhelp Entity is required to enter into a written contract or other binding legal act with any Data Controllers or Data Processors outside the Webhelp Group if they are Processing Personal Data. The above-mentioned contract or other binding legal act, shall set out the elements mentioned in Article 3.3 above 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, the obligations and rights of Webhelp and describe any technical and organisational measures required to process securely Personal Data. Such contract may include this Privacy Policy as to disclose and enforce Webhelp's Privacy Policy.

Thus, if a Webhelp Entity, acting as Data Controller or Data Processor on behalf of another Webhelp Entity, uses the services of a subcontractor which is established outside the EEA and needs for the purpose of the services being performed to share its Employees' Personal Data (only to the extent necessary for the operations), Webhelp assesses prior to the transfer that the subcontractor is able to meet the requirements of the BCR-C and frame the transfer by the appropriate binding legal act.

In case of legal obligation to share Data with the authorities, Webhelp commits to notify the relevant EEA Supervisory Authorities about this transfer without undue delay and to transfer only the necessary Personal Data. 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, indiscriminate and disproportionate way. Webhelp shall use its best efforts to circumvent prohibition to notify the relevant EEA Supervisory Authorities about a Transfer of Personal Data to authorities due to a legal obligation. Where it is not possible to circumvent such prohibition, Webhelp must provide annual general information regarding the numbers of disclosure of Personal Data to the relevant EEA Supervisory Authorities. Any notification within Webhelp and planned notification to EEA Supervisory Authorities are subject to the mechanism and provisions of Article 12.3 below.

4.10 Implementing Personal Data Breach notification measures

Where a Personal Data Breach occurs, Webhelp shall comply with the applicable Data Breach procedure adopted by Webhelp.

In any case, Webhelp and/or Webhelp Entity shall without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to (1) Webhelp SAS or to the Webhelp Entity within the EEA with delegate data protection responsibilities and other relevant Local Privacy Leaders when such Webhelp Entity is acting as a Data Controller (2) the competent EEA Supervisory Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The above-mentioned notification shall cover at least the following information:

- Nature of the Personal Data Breach and scope of the Personal Data Breach, including when possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

- Name and contact detail of the Group Data Protection Officer (“**DPO**”) or other contact point where more information can be obtained
- Describe the consequences likely to result from the Personal Data Breach;
- Describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Webhelp shall document any Personal Data Breach and the above mentioned information. Upon request, Webhelp shall make this documentation available to the competent EEA Supervisory Authority

Webhelp, when Processing Personal Data on its own behalf as a Controller within the Webhelp Group, and when Processing Personal Data on behalf of a Webhelp Entity acting as a Controller , may also need to communicate to the Data Subjects about the Personal Data Breach where it results in a high risk to the rights and freedoms of natural persons. In such circumstances, the communication shall take place without undue delay, and shall cover the above-mentioned elements as the one which would be communicated to the competent EEA Supervisory Authority.

In the event of 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, Webhelp will proceed in accordance with the Breach procedure described in **Appendix 08.1 Procedure for Personal Data Breach Notification**.

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.

Webhelp undertakes to process Sensitive Personal Data in accordance with Applicable Data Protection Legislation and where applicable any other sectorial applicable framework adopted by EEA Supervisory Authorities.

Such Processing shall be limited and specific, in particular in relation to Webhelp Employees.

Where it intends to process Sensitive Personal Data on its own behalf, Webhelp will ensure that:

- The Processing is necessary and lawful; or
- The Processing is carried out with appropriate safeguards and controls; or
- When necessary, the Data Subject has given explicit consent to the Processing of those Sensitive Personal Data for one or more specified purposes. Such consent shall not be considered as necessary when (1) the Data Subject is not in a position to give his/her consent and the Processing is necessary to protect the vital interests of the Data Subject or of another person; (2) the Data Subject itself has already manifestly rendered the affected Sensitive Personal Data part of the public domain; (3) When applicable, the Processing is explicitly permitted by Applicable Data Protection Legislation or any national law (e.g. registration/protection of minorities); or
- When necessary, the Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no grounds for assuming that the Data Subject has an overriding legitimate interest in ensuring that such data is not Processed.

6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

In the course of their business, Webhelp Entities may Transfer Personal Data to other entities of Webhelp Group or to third parties. Such entities of Webhelp and/or third parties may be located outside the European Economic Area (hereinafter “**EEA**”). In such a case, Transfers of Personal Data are deemed to take place. 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 Controller to another Webhelp Entity outside of the EEA acting either as Data Controller or as Data Processor will be supported by the provisions of this BCR-C; or
- Transfers of Personal Data from a Webhelp Entity acting as Data Controller 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; or;
- Transfers of Personal Data from a Webhelp Entity acting as Data Controller 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.

In any event, Webhelp 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.

7. RIGHTS OF DATA SUBJECT

Due to the Processing of their Personal Data by Webhelp as Data Controller or by a Webhelp Entity as a Processor Processing Personal Data on its behalf, Data Subjects are entitled to enforce this BCR-C as third-party beneficiaries

Data Subjects must at least be able to enforce the following elements:

- Purpose limitation of the Processing (Article 4.1);
- Data minimisation (Article 4.3);
- Limitation of the storage periods (Article 4.6);
- Data quality (Article 4.5);
- Data protection by design and by default and measures to ensure data security (Articles 12 and 4.7);
- Legal basis for processing (Article 4.1);
- Specific rules when processing of special categories of Personal Data (Article 5);
- Transparency and easy access to this BCR-C; (Article 12.1);
- Rights of access, rectification, erasure, restriction, objection to processing, right to data portability, right not to be subject to decisions based solely on automated processing, including profiling; (Article 7.3)
- Third-party beneficiary rights (Article 7);
- Onwards transfers (Article 4.9);
- National legislation preventing respect of BCRs (Article 12.3);
- Right to complain through the internal complaint mechanism of the companies (Appendix 5 – Article 3.1);
- Cooperation duties with EEA Supervisory Authority (Article 12.4);
- Right to lodge a complaint with the competent EEA Supervisory Authority (choice before the supervisory authority in the Member State of his habitual residence, place of work or place of the alleged infringement) and before the competent court of the EU Member State (choice for the Data Subject to act before the courts where the controller or processor has an establishment or where the Data Subject has his or her habitual residence) (Article 8);
- Right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR-C (Appendix 5 – Article 3.4.2);

Thus, Webhelp acknowledges that Data Subjects are entitled to seek judicial remedies and/or remedies before a data protection authority under the conditions defined below, for any non-compliance with this BCR-C and to receive compensation for any damages resulting from the violation of the BCR-C by any Webhelp Entity.

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

Where a Webhelp Entity within the EEA does not comply with the BCR-C, Webhelp acknowledges that the Webhelp Entity within the EEA responsible for 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-C has been infringed by Webhelp as Data Controller or by a Webhelp Entity as a Processor Processing Personal Data on its behalf. 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.

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

Where a Webhelp Entity outside of the EEA does not comply with the BCR-C, Webhelp SAS (1) endorses responsibility for any material and non-material damages resulting from the non-compliance with the BCR-C, 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 claim 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 as Data Controller or by a Webhelp Entity as a Processor Processing Personal Data on its behalf, infringes this BCR-C. 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-C 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 also discharge itself from any responsibility.

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 Webhelp Entity acting as a Data Controller or by a third party, for legitimate interests purposes, including profiling at any time, on grounds relating to their personal individual situation, unless the interests pursued by Webhelp override the interests rights and freedoms of the Data Subjects;
- Object to the Processing of their Personal Data for marketing purposes, including 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 Controller, it will handle such request without undue delay and in accordance with the complaint handling procedure specified under Section 8 below.

7.4 Exercising Data Subjects' Rights

Data Subjects are entitled to enforce this BCR-C as third-party beneficiaries, and to exercise their rights with respect to the Processing of their Personal Data by Webhelp as Data Controller. 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 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 5).

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 can seek judicial remedy as further detailed above in section 7.1 and 7.2 above.

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

- **Appendix 5 - Procedure for Data Subjects' requests where Webhelp acts as Data Controller**

8. DATA SUBJECTS COMPLAINT HANDLING PROCEDURE

Data Subjects are entitled to lodge a complaint regarding the Processing of Personal Data they consider non-compliant with this BCR-C before the Webhelp Entity they deem to be non-compliant. Where the breach is likely to result from an act of a Webhelp Entity located outside the EEA, the Data Subject can lodge the complaint directly before Webhelp SAS.

Such complaint will be handled by Webhelp in due course and with particular care and attention according to the steps and timing defined herein. Such provisions are also applicable in relation to Data Subjects requests to exercise their rights.

In practice, complaints made by Data Subjects will be handled according to the procedure defined under **Appendix 5 - Procedure for Data Subjects' requests where Webhelp acts as Data Controller**.

Webhelp commits to revert to a Data Subject with a reply to his/her complaint within one month from the date such complaint is lodged in accordance with the provisions herein.

In the event Webhelp decides to reject a complaint made by a Data Subject, Webhelp undertakes to inform such Data Subject about its decision and to provide him/her with information regarding the reason for such dismissal. In any case, Webhelp acknowledges that Data Subjects remain entitled to lodge a claim before an EEA Supervisory Authority and / or to seek judicial remedy.

In the event Webhelp considers that a complaint made by a Data Subject is justified, Webhelp commits to implement the corrective measures it deems adequate to remedy such situation as soon as reasonably possible. In addition, Webhelp will also inform the concerned Data Subject once the corrective measures have been implemented and the situation is remedied.

9. PRIVACY BY DESIGN / PRIVACY BY DEFAULT

In order to ensure that the principles defined under this BCR-C are effectively taken into account and reflected in the different Processing it carries out, Webhelp will take data protection into consideration from the very beginning of any new project.

In order to provide a high level of protection to the Personal Data within the organisation, the principles and obligations defined hereunder will thus be integrated into the design of each project on the basis of privacy by design procedures adopted by Webhelp.

10. TRANSPARENCY AND COOPERATION

12.1 Communication of the BCR-C

Webhelp will openly communicate this BCR-C 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-C 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-C through internal systems and means.

12.2 Information to Data Subjects

Webhelp, where acting as Data Controller shall provide Data Subjects any information required by the Applicable Data Protection Legislation. Webhelp will provide such information without delay and within a reasonable period after obtaining the Personal Data, but at the latest within one month, at the time of first communication or first disclosure with a legitimate recipient. Such information shall be composed at least of the following elements:

- The identity and the contact details of the Data Controller;
- The contact details of the data protection officer (DPO);
- The purposes of the Processing and its legal basis;
- If the information is not collected directly from the Data Subject, the categories of Personal Data Processed;
- The recipients of the Personal Data;
- Where applicable, the existence of Data Transfers outside of the EEA, the countries where the Personal Data is transferred to, the measures implemented to ensure an adequate level of protection and the means by which to obtain a copy of them or where they have been made available;
- The data retention period;
- The rights of the Data Subjects as defined under Article 7 above. (e.g. the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability);
- The right to lodge a complaint before a supervisory authority;
- Where Personal Data is collected from the Data Subject, whether the Data Subject (1) is obliged to provide the Personal Data due to any statutory or contractual requirement, or (2) has a requirement to provide the Personal Data as it is necessary to enter into a contract, and of the possible consequences of failure to provide such data;
- If the Processing is based on the consent of the Data Subjects, the right for them to withdraw their consent at any time without affecting the lawfulness of Processing based on consent before its withdrawal;
- If the Processing is based on Webhelp's legitimate interest, explanations regarding said legitimate interest;
- As the case may be, the existence of automated decision-making, including profiling; and
- Where the Personal Data is not collected from the Data Subject, any available information as to their source (e.g. in particular, categories of Personal Data, source from which the Personal Data originates, public nature of the Personal Data);

Webhelp undertakes to provide such information to Data Subjects in accessible, easy to understand, clear and in plain and simple language

12.3 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-C, 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) Webhelp SAS, (ii) the EU Webhelp Entity with delegated data protection responsibilities and (iii) the DPO and the relevant Local Privacy Leader / other privacy function.

Where the notification has been performed according to the above-mentioned mechanism, Webhelp SAS will notify the competent EEA Supervisory Authority. In such a 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 mandate 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 the Webhelp Entity shall use their best efforts to circumvent prohibition to notify 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, identity of the 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-C, 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-C.

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-C, 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 EU Webhelp Entity. Following the notification, the EU Webhelp Entity 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 EU Webhelp Entity shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these BCR-C. If the contract involves more than two parties, 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.

12.4 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-C.

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

11. CHANGE TO THE BCR-C

Webhelp DPO will ensure that it keeps up to date a list of entities bound by the BCR-C. Where any new entity of Webhelp becomes effectively bound by the BCR-C (as specified in Article 2.2), Webhelp DPO shall update the list and shall inform without undue delay all Webhelp Entities and relevant EEA Supervisory Authorities via the competent EEA Supervisory Authority, and such updated information will be made available to Data Subjects 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-C or on the level of protection of the rights granted by this BCR-C, Webhelp undertakes to promptly inform Webhelp Entities and EEA Supervisory Authorities.

12. 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	Procedure for Data Subjects' requests where Webhelp acts as Data Controller
Appendix 06	Not applicable to BCRs-C
Appendix 07	Not Provided
Appendix 08	Not Provided
Appendix 09	Not Provided
Appendix 10	Not Provided
Appendix 11-A	BCR-C List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)
Appendix 11-B	Not applicable to BCRs-P

Appendix 01 - A List of Webhelp Entities bound by the BCR-C and local privacy email contacts

#	Entity	Country	Privacy email contact
1.	Webhelp Albania Shpk	Albania	privacy@it.webhelp.com
2.	Webhelp Algerie SPA	Algeria	privacy@dz.webhelp.com
3.	Webhelp Australia Pty Ltd	Australia	privacy@my.webhelp.com
4.	Webhelp Austria GmbH	Austria	privacy@de.webhelp.com
5.	Webhelp Payment Services Benelux, SA	Belgium	privacy@wps.webhelp.com
6.	Webhelp Benin	Bénin	Privacy@fr.webhelp.com
7.	Webhelp BH d.o.o. Sarajevo	Bosnia-Herzegovina	privacy@de.webhelp.com
8.	Webhelp Bulgaria EOOD	Bulgaria	privacy@de.webhelp.com
9.	Les services Webhelp, Inc	Canada	protecciondedatos@onelinkbpo.com
10.	Webhelp Business Consulting (Shanghai) Co. Ltd	China	privacy@my.webhelp.com
11.	Webhelp (Suzhou) Information Technology Co. Ltd	China	privacy@my.webhelp.com

#	Entity	Country	Privacy email contact
12.	Onelink SAS	Colombia	protecciondedatos@onelinkbpo.com
13.	Onelink International SAS	Colombia	protecciondedatos@onelinkbpo.com
14.	Experts Colombia SAS	Colombia	protecciondedatos@onelinkbpo.com
15.	Getcom Colombia SAS	Colombia	protecciondedatos@onelinkbpo.com
16.	Getcom Servicios SAS	Colombia	protecciondedatos@onelinkbpo.com
17.	Webhelp Enterprise Sales Solutions, s.r.o	Czech Republic	privacy@cz.webhelp.com
18.	Webhelp Denmark, AS	Denmark	privacy@nordic.webhelp.com
19.	Webhelp Egypt	Egypt	privacy@eg.webhelp.com
20.	Onelink SA de CV	El Salvador	protecciondedatos@onelinkbpo.com
21.	Tetel SA de CV	El Salvador	protecciondedatos@onelinkbpo.com
22.	Getcom International SA de CV	El Salvador	protecciondedatos@onelinkbpo.com
23.	RH-T SA de CV	El Salvador	protecciondedatos@onelinkbpo.com
24.	Webhelp OÜ	Estonia	privacy@nordic.webhelp.com

#	Entity	Country	Privacy email contact
25.	Webhelp Finland, Oy	Finland	privacy@nordic.webhelp.com
26.	GoBeyond Partners, SAS	France	privacy@fr.webhelp.com
27.	Webhelp, SAS	France	privacy@fr.webhelp.com
28.	Webhelp Conseil, SAS	France	privacy@fr.webhelp.com
29.	W Automobile Services, SAS	France	privacy@fr.webhelp.com
30.	Webhelp France, SAS	France	privacy@fr.webhelp.com
31.	Webhelp Caen, SAS	France	privacy@fr.webhelp.com
32.	Webhelp Compiègne, SAS	France	privacy@fr.webhelp.com
33.	Webhelp Fontenay, SAS	France	privacy@fr.webhelp.com
34.	Marnix French ParentCO, SAS	France	privacy@webhelp.com
35.	Marnix French TOPCO, SAS	France	privacy@webhelp.com
36.	Marnix, SAS	France	privacy@webhelp.com
37.	WowHoldCo, SAS	France	privacy@webhelp.com

#	Entity	Country	Privacy email contact
38.	Webhelp Gray, SAS	France	privacy@fr.webhelp.com
39.	Webhelp Montceau, SAS	France	privacy@fr.webhelp.com
40.	Webhelp Saint-Avoid, SAS	France	privacy@fr.webhelp.com
41.	Webhelp Vitré, SAS	France	privacy@fr.webhelp.com
42.	Webhelp University France, SAS	France	privacy@fr.webhelp.com
43.	Webhelp Prestations, SAS	France	privacy@fr.webhelp.com
44.	Webhelp WTG, SAS	France	privacy@fr.webhelp.com
45.	DMH3, SAS	France	privacy@webhelpmedica.com privacy@patientys.com
46.	Webhelp Medica Customer Expérience	France	privacy@webhelpmedica.com privacy@patientys.com
47.	Patientys, SAS	France	privacy@webhelpmedica.com privacy@patientys.com
48.	MED-TO-MED, SAS	France	privacy@webhelpmedica.com privacy@patientys.com
49.	Webhelp Grand-Est, SAS	France	privacy@fr.webhelp.com
50.	Webhelp Medica, SAS	France	privacy@webhelpmedica.com privacy@patientys.com

#	Entity	Country	Privacy email contact
51.	Webhelp SFIA, SAS	France	privacy@fr.webhelp.com
52.	Webhelp WCS, SAS	France	privacy@fr.webhelp.com
53.	Netino, SAS	France	privacy@netino.webhelp.com
54.	Solvencia, SAS	France	privacy@wps.webhelp.com
55.	Webhelp O2C Holding, SAS	France	privacy@wps.webhelp.com
56.	Webhelp KYC Services, SAS	France	privacy@wps.webhelp.com
57.	Webhelp Payment Services France, SAS	France	privacy@wps.webhelp.com
58.	Webhelp Payment Services Deutschland, GmbH	Germany	privacy@wps.webhelp.com
59.	Webhelp Sun Holding GmbH	Germany	privacy@de.webhelp.com
60.	Webhelp Holding Germany GmbH	Germany	privacy@de.webhelp.com
61.	Webhelp Deutschland GmbH	Germany	privacy@de.webhelp.com
62.	INVIRES GmbH	Germany	privacy@de.webhelp.com
63.	RIGHTHEAD GmbH	Germany	privacy@de.webhelp.com

#	Entity	Country	Privacy email contact
64.	IQ-to-Link Gmbh	Germany	privacy@de.webhelp.com
65.	Webhelp Ghana Ltd	Ghana	<u>privacy@fr.webhelp.com</u>
66.	Webhelp Hellas Business Enterprise Sales SMLTD (MEPE in Greek)	Greece	<u>privacy@gr.webhelp.com</u>
67.	Onelink Guatemala SA	Guatemala	<u>privacy@gr.webhelp.com</u>
68.	Onelink Solutions Guatemala SA	Guatemala	<u>privacy@gr.webhelp.com</u>
69.	Inversiones Xperts Guatemala SA	Guatemala	<u>privacy@gr.webhelp.com</u>
70.	Webhelp Holding Germany GmbH (Hungary Branch)	Hungary	<u>privacy@de.webhelp.com</u>
71.	Gobeyond Partners Asia Limited	Hong Kong	privacy@my.webhelp.com
72.	Webhelp India Private Ltd	India	<u>privacy@uk.webhelp.com</u>
73.	SELLBYTEL Marketing Services India Private Ltd	India	<u>privacy@uk.webhelp.com</u>
74.	Webhelp Israel Ltd	Israel	<u>privacy@tr.webhelp.com</u>
75.	Webhelp Payment Services Italia, SRL	Italy	<u>privacy@wps.webhelp.com</u>
76.	Webhelp Payment Services France succursale Italie	Italy	<u>privacy@wps.webhelp.com</u>

#	Entity	Country	Privacy email contact
77.	Webhelp Enterprise Sales Solutions Italy	Italy	privacy@it.webhelp.com
78.	Webhelp Cote d'Ivoire	Ivory Coast	privacy@ci.webhelp.com
79.	WH Abidjan Le Workshop	Ivory Coast	privacy@ci.webhelp.com
80.	Webhelp SAS (succursale Côte d'Ivoire)	Ivory Coast	privacy@ci.webhelp.com
81.	Webhelp Japan KK	Japan	privacy@my.webhelp.com
82.	Webhelp Jordan LLC	Jordan	privacy@jo.webhelp.com
83.	IQ-to-Link shpk	Kosovo	privacy@de.webhelp.com
84.	Webhelp Kosovo L.L.C.	Kosovo	privacy@de.webhelp.com
85.	Webhelp Latvia SIA	Latvia	privacy@nordic.webhelp.com
86.	Webhelp SIA	Latvia	privacy@nordic.webhelp.com
87.	Webhelp Madagascar, SA (zone franche)	Madagascar	privacy@mg.webhelp.com
88.	Webhelp Malaysia Sdn Bhd	Malaysia	privacy@my.webhelp.com
89.	Onelink Mexico SA de CV	Mexico	protecciondedatos@onelinkbpo.com

#	Entity	Country	Privacy email contact
90.	Onelink Servicios SA de CV	Mexico	protecciondedatos@onelinkbpo.com
91.	Webhelp Maroc, SA	Morocco	privacy@ma.webhelp.com
92.	Webhelp SAS Succursale	Morocco	privacy@ma.webhelp.com
93.	Webhelp Services, SA	Morocco	privacy@ma.webhelp.com
94.	Webhelp Contact Center, SA	Morocco	privacy@ma.webhelp.com
95.	Webhelp Multimedia, SA	Morocco	privacy@ma.webhelp.com
96.	Webhelp GRC, SA	Morocco	privacy@ma.webhelp.com
97.	Webhelp Technopolis, SA	Morocco	privacy@ma.webhelp.com
98.	Webhelp University Maroc, SARL	Morocco	privacy@ma.webhelp.com
99.	Webhelp Agadir, SA	Morocco	privacy@ma.webhelp.com
100.	Webhelp Fès, SA	Morocco	privacy@ma.webhelp.com
101.	Webhelp Meknès, SA	Morocco	privacy@ma.webhelp.com
102.	Webhelp Marrakech, SA	Morocco	privacy@ma.webhelp.com

#	Entity	Country	Privacy email contact
103.	Webhelp Afrique	Morocco	privacy@ma.webhelp.com
104.	Webhelp Netherlands Holding, BV	Netherlands	privacy@nl.webhelp.com
105.	Customer Contact Management Group, BV	Netherlands	privacy@nl.webhelp.com
106.	Webhelp Nederland, BV	Netherlands	privacy@nl.webhelp.com
107.	Webhelp Enterprise BV	Netherlands	privacy@nl.webhelp.com
108.	Stacelet Holding, BV	Netherlands	privacy@nl.webhelp.com
109.	Telecats BV	Netherlands	privacy@nl.webhelp.com
110.	Customer Contact Performance Group B.V.	Netherlands	privacy@nl.webhelp.com
111.	CCPG Amsterdam B.V.	Netherlands	privacy@nl.webhelp.com
112.	CCPG Utrecht B.V.	Netherlands	privacy@nl.webhelp.com
113.	Xperts Nicaragua SA	Nicaragua	protecciondedatos@onelinkbpo.com
114.	Onelink Nicaragua SA	Nicaragua	protecciondedatos@onelinkbpo.com
115.	Onelink BPO SA	Nicaragua	protecciondedatos@onelinkbpo.com

#	Entity	Country	Privacy email contact
116.	Webhelp Company Severna Makedonija DOOEL Skopje	North-Macedonia	privacy@de.webhelp.com
117.	Webhelp Norway Consulting AS	Norway	privacy@nordic.webhelp.com
118.	Webhelp Norway, AS	Norway	privacy@nordic.webhelp.com
119.	Webhelp Peru S.A.C.	Peru	protecciondedatos@onelinkbpo.com
120.	BPO Consulting S.A.C.	Peru	protecciondedatos@onelinkbpo.com
121.	SELLBYTEL Group Philippines, Inc.	Philippines	privacy@my.webhelp.com
122.	Webhelp Poland Sp. z.o.o.	Poland	privacy@de.webhelp.com
123.	Webhelp Sun Portugal, Unipessoal, Lda	Portugal	privacy@pt.webhelp.com
124.	Webhelp Oeiras, Lda	Portugal	privacy@pt.webhelp.com
125.	Webhelp Lisbon, Unipessoal, Lda	Portugal	privacy@pt.webhelp.com
126.	Webhelp SAS Succursale em Portugal	Portugal	privacy@pt.webhelp.com
127.	Webhelp Braga LDA	Portugal	privacy@pt.webhelp.com
128.	Righthead -Empresa de Trabalho Temporario Lda	Portugal	privacy@pt.webhelp.com

#	Entity	Country	Privacy email contact
129.	WH New Generation Lisbon	Portugal	privacy@pt.webhelp.com
130.	Webhelp SFIA, Sucursal em Portugal	Portugal	privacy@pt.webhelp.com
131.	Webhelp Payment Services Espana, Sucursal em Portugal	Portugal	privacy@wps.webhelp.com
132.	Webhelp Romania SRL	Romania	privacy@ro.webhelp.com
133.	Pitech Plus SA	Romania	privacy@ro.webhelp.com
134.	MindMagnet Plus SRL	Romania	privacy@ro.webhelp.com
135.	Webhelp Senegal SAS	Senegal	privacy@sn.webhelp.com
136.	Webhelp SAS Succursale Senegal	Senegal	privacy@sn.webhelp.com
137.	Webhelp d.o.o Beograd	Serbia	privacy@de.webhelp.com
138.	Webhelp Singapore Pte Ltd	Singapore	privacy@my.webhelp.com
139.	Webhelp Slovakia, s.r.o.	Slovakia Republic	privacy@it.webhelp.com
140.	Webhelp Holding Germany GmbH (Slovenia Branch)	Slovenia	privacy@de.webhelp.com
141.	Webhelp South Africa Outsourcing Pty Ltd	South-Africa	privacy@uk.webhelp.com

#	Entity	Country	Privacy email contact
142.	Webhelp SAS, Sucursal en Espana	Spain	privacy@es.webhelp.com
143.	Direct Medica Iberica S.L.	Spain	privacy@webhelpmedica.com privacy@patientys.com
144.	Webhelp Malaga SLU	Spain	privacy@es.webhelp.com
145.	Webhelp Payment Services Espana SA	Spain	privacy@wps.webhelp.com
146.	Webhelp Spain Business Process Outsourcing S.L.	Spain	privacy@es.webhelp.com
147.	Webhelp Spain Holding SLU	Spain	privacy@es.webhelp.com
148.	Telenamic NV	Suriname	privacy@sr.webhelp.com
149.	Webhelp Sweden AB	Sweden	privacy@nordic.webhelp.com
150.	Webhelp IT Services AB	Sweden	privacy@nordic.webhelp.com
151.	Webhelp Schweiz AG	Switzerland	privacy@nordic.webhelp.com
152.	Webhelp (Thailand) Limited	Thailand	privacy@my.webhelp.com
153.	Webhelp Çağrı Merkezi ve Müşteri Hizmetleri A.Ş.	Turkey	privacy@tr.webhelp.com

#	Entity	Country	Privacy email contact
154.	Webhelp Çaęrı Merkezi ve Müşteri Hizmetleri A.Ş. Bingöl Branch	Turkey	privacy@tr.webhelp.com
155.	Webhelp Çaęrı Merkezi ve Müşteri Hizmetleri A.Ş.İzmir 2 Branch	Turkey	privacy@tr.webhelp.com
156.	Webhelp Çaęrı Merkezi ve Müşteri Hizmetleri A.Ş.Van 2 Branch	Turkey	privacy@tr.webhelp.com
157.	Webhelp Çaęrı Merkezi ve Müşteri Hizmetleri A.Ş.Ümraniye Branch	Turkey	privacy@tr.webhelp.com
158.	Webhelp Çaęrı Merkezi ve Müşteri Hizmetleri A.Ş.Bursa Branch	Turkey	privacy@tr.webhelp.com
159.	Bin Çaęrı Hizmetleri A.Ş.	Turkey	privacy@tr.webhelp.com
160.	Webhelp İnsan Kaynakları Danışmanlık ve Destek Hizmetleri A.Ş.	Turkey	privacy@tr.webhelp.com
161.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş.	Turkey	privacy@tr.webhelp.com
162.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Istanbul Kagithane Branch	Turkey	privacy@tr.webhelp.com
163.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri A.Ş. Ankara Basinevleri Branch	Turkey	privacy@tr.webhelp.com
164.	Telecom Service Centres Ltd	United-Kingdom	privacy@uk.webhelp.com
165.	Webhelp Payment Services UK Ltd	United-Kingdom	privacy@wps.webhelp.com
166.	Webhelp Medica UK Limited	United-Kingdom	privacy@webhelpmedica.com privacy@patientys.com

#	Entity	Country	Privacy email contact
			:
167.	Webhelp USA Group Inc	USA	protecciondedatos@onelinkbpo.com
168.	Webhelp USA LLC	USA	protecciondedatos@onelinkbpo.com
169.	Webhelp US LLC	USA	protecciondedatos@onelinkbpo.com
170.	Webhelp Logbox USA	USA	privacy@wps.webhelp.com
171.	Webhelp Americas LLC	USA	protecciondedatos@onelinkbpo.com
172.	Webhelp California Inc.	USA	protecciondedatos@onelinkbpo.com

Appendix 02 Definitions for BCR and Procedures

“Applicable Legislation”	Data Protection	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 Agreement”	Data Transfer	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 to 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, ransomware 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 grant 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 processing 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 Procedure for Data Subjects' requests where Webhelp acts as Data Controller

APPENDIX 5

PROCEDURE FOR HANDLING DATA SUBJECTS COMPLAINTS – CONTROLLER -

1. INTRODUCTION

The adoption of the 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 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 Controller, 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.

This document describes how Webhelp shall handle a Data Subject's Request where Webhelp acts as Data Controller (stakeholders, steps and timeline). Where the Request is received from the Data Subjects and that Personal Data is processed by Webhelp on behalf of one of Webhelp's clients, all requests shall be handled according to the procedure specifically defined under **Appendix 06 - Procedures for handling Data Subjects' requests where Webhelp acts as Data Processor**.

3. PROCEDURES

As a preliminary step, Webhelp shall expressly inform Data Subjects that they can exercise their rights in accordance with the provisions of Section 13.2 of the Privacy Policy.

3.1 Contact and acknowledgement of receipt of Request

(a) Standard procedure

Webhelp shall also specify how such rights can be exercised. For this purpose, Webhelp will provide Data Subjects with accessible means to exercise their rights and, in particular a single dedicated contact email to be used irrespective of the country a Data Subject is located in. Therefore, any Request as part of this procedure may be sent directly at the following address: privacy@webhelp.com - local emails can be used in order to take into account local specificity, such as language.

On receipt of a Request, the Group Data Protection Officer ("**DPO**"), or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall ensure they acknowledge receipt thereof no later than 3 working days after the Request was received.

(b) Exception

In the event a complaint from a Data Subject is raised through a different channel than the one described above, the Webhelp entity or function receiving the complaint shall immediately upon becoming aware, contact the DPO, and (1) internal postal services; (2) Local Privacy Leaders; (3) Business Privacy Referent; and (4) HR departments shall be informed of such procedure.

The Group Data Protection Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties shall acknowledge receipt of the matter in writing within 2 working days as from the notification by the function.

3.2 Information collection

Prior to transferring a Request internally, the Group Data Protection Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall (1) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (2), if deemed necessary, obtain as much information as possible to enable that the Request to be duly handled.

As a minimum, and to the extent possible, it shall obtain the following information ("**Minimum Information**"):

- First and last name of the Data Subject; and
- Where legally permitted/requested, copy of the Data Subject's ID or any other document required as a proof of identity; and
- Contact details to be used for reverting to the Data Subject; and
- The Personal Data concerned by the Request and the subject matter of the latter; and
- Date when Personal Data where initially collected; and
- Type of right that the Data Subject wants to exercise (please indicate whether access, deletion, blocking or correction).

If deemed necessary, Webhelp shall obtain the following information:

- Webhelp entity which initially collected the Personal Data; and
- Category of processing in relation to which the Data Subject is submitting his/her Request;
- Any relevant details regarding the Request.

In order to obtain the necessary information, Webhelp can invite the Data Subject, who has not specified sufficient information in their email, to further complete a question form, with free text field, or any other means introduced by Webhelp to facilitate the required information collection from the Data Subject. (e.g. pre-fill form field, options available through checkbox etc.). Means allowing collection of data shall, at a minimum, indicate (1) if the answer is mandatory or not and (2) the consequences if answer is not provided.

3.3 Request assessment

DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall assess if they have obtained the Minimum Information for handling the Request.

Based on the information requested and obtained, the DPO shall assess the Request. If he/she considers that the Request is reasonable and legitimate (as opposed to a Request with no proof of the Data Subject identity, an excessive demand resulting from repetitive Requests, Request of data already deleted according to the retention period, Requests on behalf of others, career forecast data, etc.) then:

The DPO shall (i) document any Request received and (ii) make the relevant assessment of the Request. In order to properly assess the Request, the DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the hereinabove duties may need to answer to the following questions:

- What is the nature of the Request? (access, deletion, opposition, rectification, portability) ;
- Do I have enough information to identify the Data Subject? ;
- Do I have enough information regarding the scope of the Request? (geographical and material scope) ;
- Does the Data Subject already have possession or easy access to the requested data (e.g., through Webhelp systems)? ;
- 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;
- Is the Data Subject Request based on a legitimate interest? ;
- Is it technically possible to address the Data Subject's Request (given in particular the volume of data at stake)? ;
- 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? If no, this Personal Data cannot be communicated to the Data Subject.

3.4 Answer type identification

On this basis, one can contemplate three different cases:

(a) **Case 1**

Where the information provided by the Data Subject is **not sufficient** to handle the Request, the DPO, or any other individual or entity, internal or external appointed by the DPO for the purpose of managing the following duties, shall send a request for additional information to the Data Subject no later than 10 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 2 months, subject to documentation of the assessment of the complexity by the DPO.

(b) **Case 2**

Where the DPO considers in their initial assessment, that the Request may **not be legitimate as described in section 3.7**, he/she shall not immediately close the case. The Group Data Protection Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties shall reply to the Data Subject within 10 working days after receiving the Request, by asking the Data Subject to provide further explanations as to why the Data Subject intends to exercise its rights.

Where necessary, the DPO may inform the relevant stakeholders at local level and the Local Privacy Leader.

Upon receipt of further justification regarding the legitimacy of the Request, the DPO, or the Local Privacy Leader shall, within 15 working days after receiving the information from the Data Subject, (1) make sure that it responds to the Request, or (2) Where he or she considers during the first analysis that the Request addressed by the Data Subject is not legitimate, document why it considers the Request not legitimate and reply to the Data Subject.

Guidance for assessing the legitimacy of the Request is provided above of such procedure. 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 to seek a judicial remedy.

Where the DPO considers that, based on the additional elements, the Request can be handled it shall ensure that it responds to the Data Subject within the above mentioned 15 working days. Where the Request is too complex and subject to compliance with any legal requirement, the timeline of the response may be extended up to 2 months, subject to documentation of the assessment of the complexity by the DPO.

(c) **Case 3**

Where information provided by the Data Subject is sufficient, the DPO shall make sure that it responds to the Request without undue delay and maximum **1 month from the receipt of the Request**.

Please note that 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 further detailed herein).

3.5 Local mandatory provisions

The Local Privacy Leader, if not directly appointed by the DPO for the purpose of managing the answers to Requests received by Webhelp, shall be ready to cooperate with the DPO by providing the latter with any relevant information in relation to the matter. The DPO shall then give guidance as to how to handle the case, by taking into account the local circumstances, within 7 working days after receiving the information from the Local Privacy Leader.

3.6 Escalation process

Where the Data Subject is not satisfied with the initial response provided by the Local Privacy Leader or the DPO, and resulting from the handling procedure described above, 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. DPO shall inform the Privacy and Data Council of such request, and allow the Privacy and Data Council to proceed to the analysis of such request.

Taking into consideration the analysis provided by the Privacy and Data Council, and without disclosing such analysis to the Data Subject, the DPO, 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.

3.7 Refusal of a Request

Although Webhelp is committed to handling Data Subject Requests efficiently, under certain circumstances, Webhelp may be entitled not to accept a Data Subject's Request.

Webhelp is entitled to decline a Data Subject's Request, where accessing the Data Subject's Request would actually or potentially mean that the following information would be shared with the Data Subject:

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

Where information/Personal Data regarding other Data Subjects is visible, data may be redacted before it is shared with the Data Subject.

In addition, where a Data Subject objects further processing of his/her Personal Data and/or asks for the deletion of his/her Personal Data, Webhelp may decline such Request where there is a legal obligation on, or an over-riding legitimate interest for, Webhelp to retain the Personal Data. This shall be assessed on a case by case basis and duly documented.

In any case, if a Data Subject Request or complaint is rejected by Webhelp or the answer does not satisfy the Data Subject, the Data Subject can contact the DPO and / or can directly lodge a complaint with its competent data protection authority.

3.8 Communication with Data Subjects

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.

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 require significant effort 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 11-A BCR-C material scope: List of Purposes of Processing and related Categories of Personal Data and Data Subjects

Appendix 11-A – Material Scope BCR-C 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-C, the table below provides further details on the transfers performed under this BCR-C. This table details on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-C. The table provided in section 1 below gives details about the transfers of personal data carried out between Webhelp Entities listed in Appendix 1 under this BCR-C. The countries to which the personal data may be transferred depend on the localization of Webhelp Entities involved in the processing activities and is provided in Appendix 1. Note that as regard BCR-C, transfers of personal data mostly occur between the Webhelp entities of a same Webhelp Region (except for the Global entities where there may be transfers between such Global entities and all other Webhelp entities depending on the Purposes of Processing. For more transparency, we have included an additional table presenting the Webhelp Regions in section 2 of the present Appendix.

1. Table on Transfers of Personal Data between Webhelp Entities listed in Appendix 1 under this BCR-C

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
HR processing activities	Recruitment management	1. Identification data (e.g., Name, Last name, E-Mail, Phone number, picture (if provided), Address) 2. Economic and financial data (e.g., salary expectation) 3. Professional data (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary)) 4. Background check (results of background check (only the results, and for successful candidates to be hired))	Candidates
	Employee records management (incl. Onboarding process, maintenance of employee record in accordance with the applicable legislation, administrative follow-up of occupational medicine, internal directory)	1. Identification data (e.g., Name, Last name, E-Mail, Phone number, picture of the data subject, Address, Gender, family status) 2. Professional data (e.g., CV-Resume, Educational records and information regarding skills of the employee, Previous experience, Diplomas/certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), Employee internal identification number, office location, previous work history, Business Unit Division Line Reporting Manager, contract type) 3. Economic and financial data (e.g., Income/Salary, IBAN/BIC) 4. Sensitive data (social security number)	Webhelp's employees

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Payroll Management	<p>1. Identification data (e.g., Name, Last name, E-Mail, Phone number, Address)</p> <p>2. Professional data (e.g., Employee internal identification number, contract type, hours of work)</p> <p>3. Economic and financial data (e.g., Payment data (worked hours, absences, compensation and benefits, bonus, Benefits and Entitlements Data), salary wage, IBAN/BIC,)</p> <p>4. Sensitive data (Social Security number)</p>	Webhelp's employees
	Referral Program management	<p>1. Identification data (e.g., Name, Last name, E-Mail, Phone number, Address).</p> <p>2. Professional data (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings).</p>	Webhelp's employees Candidates
	Badge management for employees	<p>1. Identification data (e.g., Name, last name, phone number)</p> <p>2. Professional data (e.g., job title role, Employee internal identification number), Employee badge number, authorized areas and working hours)</p> <p>3. Economic and financial data (e.g., payment attached to the use of the canteen)</p>	Webhelp's employees
	Employee's training management (incl. Internal WH training and client's training)	<p>1. Identification data (e.g., Name, Last name, E-Mail, Phone number, Address)</p> <p>2. Professional data (e.g., Job title role, Employee internal identification number, Training information (type of training, date, attendance, quiz results, etc.), office location, previous work history Business Unit Division, line Reporting Manager)</p>	Webhelp's employees
	Employee's career and mobility management	<p>1. Identification data (e.g., Name, Last name . E-Mail, Phone number, picture (if provided), Address)</p> <p>2. Professional data (e.g., CV-resume, Current job title role, Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary))</p>	Webhelp's employees

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Employees' background check	1. Identification data (e.g., Name, Last name, E-Mail, Phone number, photo (if provided), Address) 2. Professional data (e.g., CV-resume, Current job title role, Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary)) 4. Background check information (e.g., background check results)	Webhelp's employees
	Employees' absence and working time management	1. Identification data (e.g., Name, Last name) 2. Professional data (e.g., Employee internal identification number, office location, previous work history, Business Unit Division Line Reporting Manager, contract type, hours of work, work schedule, absences (sick leaves, vacations, etc.))	Webhelp's employees
	Professional elections management	1. Identification data (e.g., Name, Last name, age) 2. Professional data (e.g., Preparation of the electoral list (identity of voters, age, seniority, college), applications management (identity, nature of the mandate applied for, information allowing to verify compliance with eligibility requirements, if applicable trade-union membership declared by the candidates) and release of the results of the elections (identity of the candidates, mandates concerned, number and percentage of votes obtained, identity of the elected employees and, if applicable, trade-union membership of the elected employees).	Webhelp's employees
	Management of Employees representative bodies' committees	1. Identification data (e.g., Name, Last name) 2. Professional data (e.g., Convocations, preparatory documents, reports, various minutes of representative bodies' committee).	Webhelp's employees

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Employees' performance and evaluation management	<p>1. Identification data (e.g., Name, Last name).</p> <p>2. Professional data (e.g., information on evaluation: dates of the evaluation interviews, identity of the evaluator, professional competencies of the employee, objectives assigned, results objectives, results obtained, assessment of professional skills on the basis of objective criteria with a direct and necessary link to the job, observations and wishes formulated by the employee, career development forecasts. For agents, transcription of call conversation with end customer may be used for quality assessment purposes).</p>	Webhelp's employees
	Quality assessment of agents / operators	<p>1. Identification data (e.g., Name, Last name, email)</p> <p>2. Professional data (e.g., Employee internal identification number, job title role, Line reporting managers, KPIs, objectives assigned, results objectives, results obtained, assessment of professional skills on the basis of objective criteria with a direct and necessary link to the job, observations and wishes formulated by the employee, career development forecasts. transcription of call conversation with end customer may be used for quality assessment purposes, evaluation results)</p>	Webhelp's agents/operators
	Impact sourcing program management (recruitment, reporting, etc.)	<p>1. Identification data (e.g., Name, Last name . E-Mail, Phone number, photo (if provided), Address)</p> <p>2. Economic and financial data (e.g., salary expectation)</p> <p>3. Professional data (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), source of recruitment)</p>	Candidates, Webhelp's employees
	Travel and expenses management	<p>1. Identification data (e.g., Name, Last name, Address)</p> <p>2. Professional data (e.g., Job title role, employee internal identification number, booking reservation, dates of travel, business justification, line reporting manager)</p> <p>3. Economic and financial data (e.g., expenses report, invoices, IBAN / BIC)</p>	Webhelp's employees

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Social & cultural activities management	1. Identification data (e.g., Name, Last name, Address, marital status/relationship) 2. Professional data (e.g., Job title role, employee internal identification number) 3. Economic and financial data (e.g., income, benefits and benefits claimed and provided)	Webhelp's employees (and their declared relatives)
Company life & services	IT Management (IT equipment allocation and management, service desk)	1. Identification data (e.g., Name, Last name email address) 2. Professional data (e.g., employee internal identification number, job title role, office location, line reporting manager, IT request information (Ticket number, request topic, request follow-up)) 3 Technical and connection data (e.g., IP Address, user account information, Device ID, , necessary professional applications and websites)	Webhelp's employees
	Internal Information Security (Fraud Prevention)	1. Identification data (e.g., Name, Last name email address) 2. Professional data (e.g., employee internal identification number, job title role, office location, line reporting manager) 3 Technical and connection data (e.g., IP Address, user account information, Device ID, alter, results of alerts)	Webhelp Employees
	CCTV within Webhelp facilities	1. Identification data (e.g. footages)	Webhelp's employees Visitors to Webhelp's premises
	Management of telephony in the workplace	1. Identification data: (e.g. name, last name, email address, phone number) 2. Technical and connection data (e.g., IP Address, Logins, Device ID data, type of phone, relevant information regarding the use of telephony services and data necessary for invoicing purposes, including operator, the nature of the call (local, national, international), the duration of the call, the time and date of the beginning and end of the phone call and the invoice)	Webhelp's employees

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Internal communication to Employees (incl., internal communication by email, or via Virtual private networks (intranet))	1. Identification data (e.g., Name, Last name email address). 2. Professional data (e.g., charts, discussion areas, information areas applications and networks) 4. Technical and connection data (e.g., IP Address, Device ID data, user account information)	Webhelp's employees
	Employees Survey and form	1. Identification data (e.g., Name, Last name email address, phone number) 2. Technical and connection data (e.g., employee internal identification number, job title role, office location, anonymous & aggregated results)	Webhelp's employees
	Internal Directory & Employees' user access and accounts management	1. Identification data (e.g., Name, Last name email address). 2. Professional data (e.g., charts, discussion areas, information areas applications and networks). 3. Technical and connection data (e.g., IP Address, Device ID data, user account information)	Webhelp's employees
	Internet access and control and prevention of data loss	1. Identification data (e.g., Name, Last name email address) 2. Professional data (e.g., employee internal identification number, job title role, office location, line reporting manager, authorized application & website, employee job title role) 4. Technical and connection data (e.g., IP Address, Device ID data, user account information)	Webhelp's employees
Legal / Compliance	Fraud Prevention and detection	1. Identification data (e.g., Name, Last name, email, phone number). 2. Technical and connection data (e.g., IP Address, Logins ,Device ID data, interaction data, bug reports, monitoring information embedded in the application, device used). 3. Interaction data necessary to investigate a potential fraud (e.g., Identification through the means used to provide the services and contact the End Customers; Voice data of the End Client and the Service Provider's employee, transcription of the interaction. Telephone number, email address, operations planning, operations performance indicators and peer performance indicators)	Webhelp's employees Webhelp customers/clients

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Whistleblowing system	<p>1. Identification data (e.g., name last name, email, phone number, details of the people author of the alert, of the people subject of the alert and of people involved in the processing of the alert)</p> <p>2. Professional data (e.g., contract type, job title role, Function/job of the person(s) reporting the incident, the person(s) implicated in the incident and the person(s) involved in the investigation)</p> <p>3. Information of the alert (e.g., facts reported, evidence as part of the investigation, record of investigations follow-up of the alert).</p>	Webhelp's employees and administrators
	Corporate & Legal entities management <i>(incl. Mandates and proxy, Delegation of powers and signatures, Corporate reporting (boards, committees), Professional associations, external counsels directory)</i>	<p>1. Identification data (e.g., Name or company name, E-Mail , Phone number)</p> <p>2. Professional data (e.g., (e.g., CV-Resume , Educational records and information regarding skills of the employee, Previous experience, Diplomas/certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), Employee internal identification number, office location, delegation of authorities, proxy)</p> <p>3. Economic and financial data (e.g., Payment ,Income/Salary, Financial situation ,invoices, Credit card number ,IBAN / BIC)</p>	Webhelp's employees and administrators
	Employees' litigation and disciplinary procedures	<p>1. Identification data (e.g., Name, Last name, E-Mail, Phone number, footage (if necessary), Address)</p> <p>2. Professional data (e.g., employee internal identification number, office location, line reporting manager, information related to potential disciplinary actions and procedure for employees, nature of litigation for business related litigation, job title role / function)</p> <p>Information related to the litigation matter (e.g., subject matter, estimated risks, evidence, etc.)</p>	Webhelp's employees Attorneys

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Litigation management	1. Identification data (e.g., Name, Last name, E-Mail , Phone number, footage (if necessary), Address) 2. Professional data (e.g., nature of litigation for business related litigation, job title role / function) Information related to the litigation matter (e.g., subject matter, estimated risks, evidence, etc.)	Webhelp's employees Webhelp's business partners Attorneys
	Clients and business partners database (BtoB)	1. Identification data (e.g., Name or company name, E-Mail, Phone number, Address Of headquarters) 2. Professional data (e.g., job title role) 3. Economic and financial data (e.g., Payment ,Income/Salary, Financial situation, invoices, Credit card number ,IBAN / BIC)	Webhelp's Business partners/ Clients
Operation & Marketing	Client and prospect leads management	1. Identification data (Name, Last name, E-Mail, Phone number, professional Address) 2. Professional data (job title, role, company name, office location) 3. Economic and financial data (client agreement, invoice, dunning, purchase orders).	Webhelp's Clients/Prospects (business contact)
	WH Direct marketing campaigns	1. Identification data (Name, Last name, E-Mai, Phone number, professional Address) 2. Professional data (job title, role, company name, office location, optout decision)	Webhelp's Clients/Prospects (business contact)
	Processing of Payment Services - WPS	1. Identification data (e.g. Name, Last name ,ID card, E-Mail , Phone number, Postal Address , Gender, internal references) 2. Professional data (e.g., Information related to the profession, information related to the regulatory qualification of a politically exposed person) 3. Economic and financial data (e.g. Payment, Income/Salary, Financial situation, invoices, IBAN / BIC)	Webhelp's Clients/Prospects
Partner/Vendor relationships	Suppliers Management and Contract Management	1. Identification data (e.g.,Name , E-Mail , Phone number, Address Of headquarters) 2. Professional data (e.g., Job titles, copy of supplier agreements, invoice, dunning, purchase orders)	Webhelp's employees Supplier's Business contact

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	* Categories of Data Subjects
	Data broker relationship management	1. Identification data (e.g., Name, E-Mail, Phone number, address) 2. Professional data (e.g., Job title role, line reporting manager, optin/optout, hobbies, contractual relationship, invoice, dunning)	Webhelp's employees Data broker's Business contact Webhelp Client/Prospect (business contact)

2. Table on Webhelp's Regions

Webhelp Regions	Countries included in the Webhelp Region
Group (Global)	All countries* <i>*Transfers may occur between French Global entities and all other Webhelp entities of the Group, whatever their country of location identified in Appendix 1</i>
AMERICAS	Canada Colombia El Salvador Guatemala Honduras Mexico Nicaragua Peru Puerto Rico US
CRIT	Albania Czech Republic Italy Slovakia
FRANCE	Algeria Benin France Greece Ivory Coast Madagascar Morocco Portugal Romania Senegal Spain * <i>(Transfer may occur between Webhelp entities of the FRANCE Region and one French branch located in Spain attached to this region)</i>
APAC	Australia China Japan Malaysia Philippines Singapore Thailand
DACH	Austria Germany Kosovo Poland Slovenia* <i>(Transfer may occur between Webhelp entities of the DACH Region and one German branch located in Slovenia attached to this region)</i> Switzerland

Webhelp Regions	Countries included in the Webhelp Region
NETHERLANDS	The Netherlands Belgium France <i>(Transfer may occur between Webhelp entities of the Netherlands Region and one legal entity located in France attached to this region)</i> Surinam
NORDICS	Denmark Estonia Finland Latvia Lithuania Norway Spain* <i>(Transfer may occur between Webhelp entities of the NORDICS Region and one Spanish entity attached to this region).</i> Sweden
SPAIN	Spain
UK	India Sout Africa United Kingdom
TURKEY	Egypt Israel Jordan Saudi Arabia Turkey
WPS/WKS	Belgium France Germany Italy Portugal Spain United Kingdom United States <i>Transfers may occur between WPS/WKS affiliates only.</i>
NETINO	France
MSF	France
WEBHELP MEDICA	France Portugal Spain <i>Transfers may occur between Webhelp Medica affiliates only.</i>