



Webhelp

PRIVACY POLICY

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivPol-01
Version	V0.4
Approved	31/10/2018

Date	Version	Comments

TABLE OF CONTENT

1. Introduction	4
2. Scope	5
2.1 THIS EMPLOYEE PRIVACY	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 CLIENTS	6
3.4 TOWARDS WEBHELP'S DATA PROCESSORS	6
4. Principles for processing personal data	7
4.1 WHERE WEBHELP IS ACTING AS DATA CONTROLLER	7
4.1.1 DEFINING A LEGAL BASIS FOR PROCESSING	7
4.1.2 DEFINING A PURPOSE	7
4.1.3 MINIMISING PERSONAL DATA COLLECTION	7
4.1.4 HOLDING A RECORD	7
4.1.5 ACCURACY OF THE PERSONAL DATA	8
4.1.6 DEFINING A DATA RETENTION PERIOD	8
4.1.7 IMPLEMENTING SECURITY MEASURES	8
4.1.8 DATA PROTECTION IMPACT ASSESSMENT	8
4.1.9 TRANSFERS OUTSIDE THE WEBHELP GROUP	9
4.1.10 IMPLEMENTING PERSONAL DATA BREACH NOTIFICATION MEASURES	9
4.2 WHERE WEBHELP IS ACTING AS DATA PROCESSOR	10
4.2.1 TRANSPARENCY AND FAIRNESS	10
4.2.2 PURPOSE LIMITATION	10
4.2.3 DATA QUALITY	11
4.2.4 RECORD OF PROCESSING ACTIVITIES	11
4.2.5 SECURITY	11
4.2.6 RIGHTS OF THE DATA SUBJECTS	11
4.2.7 SUB-PROCESSING AND ONWARD TRANSFERS	11
5. Processing sensitive data	13
5.1 Where Webhelp is acting as Data Controller	13
5.2 Where Webhelp is acting as Data Processor	13
6. Transfer of personal data to third countries	14
7. Rights of data subjects	15
7.1 DATA SUBJECTS' RIGHTS WHERE WEBHELP ACTS AS DATA CONTROLLER	15
7.1.1 WHERE A WEBHELP ENTITY WITHIN THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY	16
7.1.2 WHERE A WEBHELP ENTITY OUTSIDE OF THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY	16
7.2 DATA SUBJECT RIGHTS WHERE WEBHELP ACTS AS DATA PROCESSOR	16
7.2.1 WHERE A WEBHELP ENTITY WITHIN THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY	17
7.2.2 WHERE A WEBHELP ENTITY OUTSIDE OF THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY	17

TABLE OF CONTENT

7.3	<i>DATA SUBJECTS' RIGHTS</i>	18
7.4	<i>EXERCISING DATA SUBJECTS' RIGHTS</i>	18
8.	Data subjects complaint handling procedure	20
8.1	<i>HANDLING DATA SUBJECTS' COMPLAINTS WHEN ACTING AS DATA CONTROLLER</i>	20
8.2	<i>HANDLING DATA SUBJECTS' COMPLAINTS WHEN ACTING AS DATA PROCESSOR</i>	20
9.	External clients' complaints	21
10.	Data protection governance	22
11.	Training and awareness	23
12.	Privacy by design/privacy by default	24
13.	Transparency and cooperation	25
13.1	<i>COMMUNICATION OF THE PRIVACY POLICY</i>	25
13.2	<i>INFORMATION TO DATA SUBJECTS</i>	25
13.3	<i>INCOMPATIBILITIES WITH LOCAL LEGISLATIONS</i>	26
13.4	<i>DUTY TO COOPERATE</i>	26
14.	Audit	27
15.	Changes to the privacy policy	28

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 this Privacy Policy (hereinafter, the “Privacy Policy”) 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 and on behalf of its Clients by the implementation of appropriate technical, physical and administrative measures and controls. 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.

As a consequence of the above and taking into consideration standards, regulations and laws applicable in the field of data protection, and the requirements introduced by the European Regulation 2016/679 adopted on 27th April 2016 (hereinafter, the “**EU Regulation**”) Webhelp will process 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 Privacy Policy 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 Privacy Policy. Furthermore, Webhelp may make available specific, local or sectorial policies. Should there be a contradiction between this Privacy Policy and such specific, local or sectorial policies, the terms of the Privacy Policy shall prevail.

As the Privacy Policy 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 Privacy Policy. As a consequence, local legislation shall be considered as an enforceable exception to this Privacy Policy and will be recorded accordingly.



2. Scope

2.1 THIS EMPLOYEE PRIVACY

This Privacy Policy is applicable whenever a Webhelp Entity Processes Personal Data as Data Controller and/or as Data Processor.

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

- Data relating to personal life;
- Economic and financial data;
- Health related data;
- Identification data;
- Pseudonymised data;
- Sensitive Personal Data;
- Technical data; or
- Transactional data.

Notwithstanding the above, this Privacy Policy applies to the Processing of Personal Data by Webhelp irrespective of its category, its nature or the status of Webhelp acting as a Data Controller or as a Data Processor.

Webhelp is also the controller of the personal data of its employees as their employer. When processing personal data of Webhelp employees, Webhelp will comply with this Privacy Policy 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 organisation where Personal Data are being Processed. Consequently, all Webhelp Entities, whatever their location or legal jurisdiction, are subject to this Privacy Policy. No transfer of Personal Data shall be carried out by any Entity of Webhelp bound by this Privacy Policy to an Entity not bound by this Privacy Policy unless such 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 Privacy Policy and ensure the protection of the rights of the Data Subjects. The Webhelp Entity bound by the Privacy Policy 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 Privacy Policy. As protecting Personal Data is a matter of individual and organisational commitment, each employee must also comply with the requirements specified under this Privacy Policy.

As such, the Privacy Policy 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 Privacy Policy 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 Privacy Policy and will comply with the requirements specified herein.

For this reason, this Privacy Policy is binding upon all the entities of the Webhelp Group by signing this Privacy Policy.

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

3.3 TOWARDS WEBHELP'S CLIENTS

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

Any Processing activity of Webhelp shall be governed by a written contract or other binding legal act, and shall set out (amongst other things) the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Data Controller.

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

3.4 TOWARDS WEBHELP'S DATA PROCESSORS

Where Webhelp engages another Data Processor such as another Webhelp Entity or 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 Privacy Policy, and if necessary the Service Agreement between Webhelp and a Data Controller.

Data Processor will process Personal Data only on Data Controller documented instructions. Any Processing activity undertaken by Webhelp's Data Processors shall be governed by a written contract or other binding legal act, and shall set out 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.



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 whether it is acting as Data Controller or as Data Processor

4.1 WHERE WEBHELP IS ACTING AS DATA CONTROLLER

4.1.1 DEFINING A LEGAL BASIS FOR PROCESSING

When Personal Data is being Processed, it is required that such Processing relies upon an appropriate legal basis, 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.

4.1.2 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.

4.1.3 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.

4.1.4 HOLDING A RECORD

When acting as a controller, Webhelp shall maintain a record of all categories of 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.



4.1.5 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, are erased or rectified.

4.1.6 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.

4.1.7 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 complies 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.

4.1.8 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 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, in particular using new technologies, is likely to result in a high Risk to the rights and freedoms of Data Subjects, Webhelp shall, 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.

Where a Data Protection Impact Assessment 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 Supervisory Authority before carrying out this Processing.



4.1.9 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 in such a manner that the Processing will meet the requirements of this Privacy Policy.

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 (amongst other things) 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.

In case of legal obligation to share Data with the authorities, Webhelp commits to notify the relevant Data Protection authority about this transfer without undue delay and to transfer only the necessary 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 Data Protection 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 authorities.

4.1.10 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 delegates data protection responsibilities when such Webhelp entity is acting as a Data Controller, or to the Data controller when such Webhelp entity acting as a Data processor of Webhelp (2) the competent 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, when Processing Personal Data on its own behalf (Data 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 data protection authority.



4.2 WHERE WEBHELP IS ACTING AS DATA PROCESSOR

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

4.2.1 TRANSPARENCY AND FAIRNESS

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

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

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

Moreover, where a Webhelp Entity has reasons to believe that its applicable legislation prevents this Webhelp Entity from fulfilling its obligations under this Privacy Policy or has substantial effect on the guarantees provided by the rules, this Webhelp Entity will promptly inform the DPO and Webhelp and the other relevant Local Privacy Leader (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation)

4.2.2 PURPOSE LIMITATION

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

- More particularly, Webhelp undertakes to process Personal Data on behalf of its Client:
- for the sole purposes expressed by such Client;
- under the conditions agreed between Webhelp and its Client under the Service Agreement; and
- for no longer than what is expressly prescribed by the Client of Webhelp.

In the event Webhelp would not be able to provide such compliance, it undertakes to promptly inform its Clients of its inability to comply. Such information from Webhelp to its Client shall be made without delay and as soon as Webhelp is aware that such compliance is not reachable. In such a case, the Clients would then be entitled to suspend the transfer of Personal Data to Webhelp.



4.2.3 DATA QUALITY

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

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

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

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

4.2.4 RECORD OF PROCESSING ACTIVITIES

When acting as a Processor, Webhelp shall maintain a record of all categories of Processing activities carried out on behalf of a controller, containing:

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

4.2.5 SECURITY

Where acting as Data Processor, Webhelp commits to comply with security and organisational measures meeting at least the requirements of the Applicable Data Protection Legislation and any existing particular measures specified in the Service Agreement with the Client.

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

4.2.6 RIGHTS OF THE DATA SUBJECTS

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

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

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

4.2.7 SUB-PROCESSING AND ONWARD TRANSFERS

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

Webhelp will not use a sub-processor without having first a written authorization from the Controller. When given a general authorisation to use sub-processors, Webhelp will inform the Client of any intended changes concerning the addition or replacement of any Sub-Processor and shall give the Client the opportunity to object to such changes as described here after and in Webhelp Data Processing Agreement.



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

In case of a legal obligation to share Data with the authorities, the involved Webhelp Entity must notify Webhelp. Webhelp commits to notify the relevant Data Protection authority and where possible the Client about this disclosure without undue delay and to comply with the Data minimisation principle. Webhelp shall precise which Data Subjects are concerned by the disclosure, which authority is asking for this disclosure and on which legal basis it is based on. In any case, Webhelp entities commit not to transfer Personal Data to public authorities in a massive and disproportionate way. In that same case, Webhelp commits to notify the Client about the disclosure.

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



5. Processing sensitive data

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

5.1 Where Webhelp is acting as Data Controller

Webhelp undertakes to process Sensitive Personal Data in accordance with any Applicable Data Protection Legislation or any other sectorial applicable Legislation.

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

5.2 Where Webhelp is acting as Data Processor

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

It will be Webhelp's Client responsibility to define what measures should be implemented in this respect and to ensure that the requirements of the Applicable Data Protection Legislation or any national law are met.

For sake of clarity, where it processes Sensitive Personal Data as Data Processor, Webhelp shall in no event be responsible for ensuring that the Processing relies on one of the legal bases defined under the above sub-section.



6. Transfer of personal data to third countries

In the course of their business, Webhelp Entities may process Personal Data on behalf of Webhelp or on behalf of its or their Clients. Such Webhelp Entities 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 either as Data Controller or as Data Processor on behalf of its Client, 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 Privacy Policy; or

- Transfers of Personal Data from a Client acting as Data Controller and located within the EEA to a Webhelp Entity outside of the EEA shall be supported by this Privacy Policy; 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 the applicable standard contractual clauses adopted by the competent supervisory authority and/or the EU Commission; or
- Transfers of Personal Data from a Webhelp Entity acting as Data Controller to third parties located outside of the EEA as Data Controller will be supported by the applicable standard contractual clauses adopted by the competent 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 will be granted to the Personal Data transferred.

7. Rights of data subjects

7.1 DATA SUBJECTS' RIGHTS WHERE WEBHELP ACTS AS DATA CONTROLLER

Due to the Processing of their Personal Data by Webhelp as Data Controller, Data Subjects are entitled to enforce this Privacy Policy as third-party beneficiaries, subject to local applicable law.

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

- Purpose limitation of the Processing (Article 4.1.1);
- Data minimisation (Article 4.1.3);
- Limitation of the storage periods (Article 4.1.6);
- Data quality (Article 4.1.5);
- Data protection by design and by default and measures to ensure data security (Articles 12 and 4.1.7);
- Legal basis for processing (Article 4.1.1);
- Specific rules when processing of special categories of Personal Data (Article 5.1);
- Transparency and easy access to this Privacy Policy; (Article 13.1);
- Rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling; (Article 7.3)
- National legislation preventing respect of BCRs (Article 13.3);
- Right to complain through the internal complaint mechanism of the companies (Appendix 5 – Article 3.1);
- Cooperation duties with Data Protection Authority (Article 13.4);
- Right to lodge a complaint with the competent 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 Privacy Policy (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 Privacy Policy and to receive compensation for any damages resulting from the violation of the Privacy Policy by any Webhelp Entity.



7.1.1 WHERE A WEBHELP ENTITY WITHIN THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY

Where a Webhelp Entity within the EEA does not comply with the Privacy Policy, 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 a 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 Privacy Policy has been infringed by Webhelp as Data Controller. 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.

7.1.2 WHERE A WEBHELP ENTITY OUTSIDE OF THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY

Where a Webhelp Entity outside of the EEA does not comply with the Privacy Policy, Webhelp SAS (1) accepts and acknowledges responsibility for any material and non-material damages resulting from the non-compliance and (2) agrees to take the necessary actions in order to remedy the acts of such other Webhelp Entity.

In such circumstances, Webhelp 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;
- subject to local applicable law the right to an effective judicial remedy where he or she claims that this Privacy Policy has been infringed by any Webhelp Entity as Data Controller and such infringement has harmed the Data Subject.

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 Privacy Policy 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.

7.2 DATA SUBJECT RIGHTS WHERE WEBHELP ACTS AS DATA PROCESSOR

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

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

- Duty to respect the instructions from the controller regarding the Data Processing including for data transfers to third countries (Article 4.2.2);
- Duty to implement appropriate technical and organisational security measures and duty to notify any Personal Data Breach to the controller (Article 4.2.5);
- Duty to respect the conditions when engaging a sub-processor either within or outside the Webhelp group (Article 4.2.8);
- Duty to cooperate with and assist the controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Article 4.2.1);
- Easy access to the Privacy Policy on Webhelp website at www.webhelp.com;
- Right to complain through internal complaint mechanisms (Article 8);
- Duty to cooperate with the supervisory authority (article 13.4);
- Liability, compensation and jurisdiction provisions (Article 9);
- National legislation preventing respect of the Privacy Policy (Article 4.2.1).



In any case, Data Subjects are:

- Entitled to seek judicial remedies for any breach of the rights guaranteed under this Privacy Policy and/or (Article 9);
- Entitled to obtain redress and where appropriate receive compensation for a damage (including material harm but also any distress) resulting from the violation of the Privacy Policy by any Webhelp Entity (Article 9);
- Entitled to lodge a complaint before the data protection authority or courts competent for the Client located in the EEA (Articles 7.2.1. and 7.2.2).

In the event where it can be evidenced that the Client has factually disappeared or no longer exists in law or has become insolvent and that no other entity has assumed the legal obligations to recover the Client's obligations, Data Subjects are hereby expressly entitled to exercise their rights under article 7.1 of this Privacy Policy and to bring a claim directly against the Webhelp Entity acting as Data Processor and bound by a Service Agreement with the Client.

7.2.1 WHERE A WEBHELP ENTITY WITHIN THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY

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

Webhelp also acknowledges that the Data Subject shall be entitled to

- lodge a complaint with a 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 Privacy Policy has been infringed by Webhelp as Data Processor. Webhelp acknowledges that such claim can be brought either before the member state where the Webhelp Entity responsible of the non-compliance is established or before the court where the Data Subject has his or her habitual place of residence.

7.2.2 WHERE A WEBHELP ENTITY OUTSIDE OF THE EEA DOES NOT COMPLY WITH THE PRIVACY POLICY

Where a Webhelp Entity outside of the EEA does not comply with the Privacy Policy, Webhelp SAS (1) accepts and acknowledges responsibility for any damages resulting from the non-compliance and (2) agrees to take the necessary actions in order to remedy the acts of such other Webhelp Entity.

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

- lodge a complaint with a data protection authority where he/she has his/her place of residence, place of work or where the Webhelp Entity with delegated responsibility is established. And/or;
- subject to local applicable law the right to an effective judicial remedy where he or she claims that this Privacy Policy has been infringed by any Webhelp Entity acting as Data Processor

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 Privacy Policy and which has resulted in the Data Subject claiming damages. In the event Webhelp SAS can demonstrate that the other Webhelp Entity located outside the EEA was not responsible for the act, then it can discharge itself from any responsibility.



7.3 DATA SUBJECTS' RIGHTS

Pursuant to the Applicable Data Protection Legislation, 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 at any time, unless such Processing is required by applicable law and provided that the Data Subject demonstrates that he/she has a legitimate ground relating to his/her particular situation; 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.

Where Webhelp is acting as Data Processor and receives a request from Data Subjects to exercise their rights, Webhelp shall inform its Client and the latter shall respond to the request. Webhelp shall only be responsible for following its Client's further instructions regarding how to handle such request. Where the Client has disappeared, or has ceased to exist or has become insolvent, Webhelp shall then handle such request directly to the extent possible and in accordance with the procedure it has adopted.

7.4 EXERCISING DATA SUBJECTS' RIGHTS

Data Subjects are entitled to enforce this Privacy Policy as third-party beneficiaries, subject to Applicable Data Protection Legislation, and to exercise their rights with respect to the Processing of their Personal Data by Webhelp, whether as Data Controller or as Data Processor. Webhelp shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner.

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.

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 and 6).

Where the Data Subject is not satisfied with the initial response provided by Webhelp such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined. Data Subject shall provide to Webhelp a detailed explanation of the unsatisfactory provisions of the solution previously provided. Webhelp shall take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

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.

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

- **Appendix 5 - Procedure for Data Subjects' requests where Webhelp acts as Data Controller**
- **Appendix 6 - Procedure for Data Subjects' requests where Webhelp acts as Data Processor**



8. Data subjects complaint handling procedure

8.1 HANDLING DATA SUBJECTS' COMPLAINTS WHEN ACTING AS DATA CONTROLLER

Data Subjects are entitled to lodge a complaint regarding the Processing of Personal Data they consider non-compliant with this Privacy Policy 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 to access, update or delete their Personal Data.

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 such a case, Webhelp acknowledges that Data Subjects remain entitled to lodge a claim before a court and/or data protection authority.

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.

8.2 HANDLING DATA SUBJECTS' COMPLAINTS WHEN ACTING AS DATA PROCESSOR

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

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

Webhelp is not responsible for handling complaints made by Data Subjects when acting as Data Processor. However, in the event the Client has factually disappeared, ceased to exist in law or become insolvent, then Webhelp undertakes to handle complaints from Data Subjects pursuant to the same procedure as specified under Section 8.1.



9. External clients' complaints

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



10. Data protection gouvernance

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

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

11. Training and awareness

Protecting Personal Data is not only a matter of compliance with privacy laws, but is part of the embodiment of Webhelp's core values. In this context, fostering a privacy culture within the group is essential to make all employees, trainees, and other persons whose conduct, in the performance of work is under the direct control of Webhelp accountable for the protection of Personal Data Processed as part of Webhelp's operations.

Therefore, this Privacy Policy shall be properly implemented within the whole organisation. To this end, Webhelp has adopted a privacy training program which aims at ensuring that Webhelp employees, trainees, and other persons whose conduct, in the performance of work is under the direct control of Webhelp, are actually aware of the obligations, principles and procedures specified under this Privacy Policy.

Such training is aimed at: (i) individuals having permanent or regular access to Personal Data; (ii) individuals involved in the collection of Personal Data; and/or (iii) individuals involved in the development of tools used to process Personal Data.

The training program will aim at providing:

- A basic level core of knowledge regarding the applicable principles when Processing Personal Data and a good understanding of the existing procedures and their implementation; and,
- Specific training adapted to the different functions within the organisation.



12. Privacy by design/privacy by default

In order to ensure that the principles defined under this Privacy Policy 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.

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

13. Transparency and cooperation

13.1 COMMUNICATION OF THE PRIVACY POLICY

Webhelp will openly communicate this Privacy Policy 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 Privacy Policy 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 Privacy Policy through internal systems and means.

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

13.2 INFORMATION TO DATA SUBJECTS

Webhelp, where active as Data Controller shall provide Data Subjects any information required by the Applicable Data Protection Legislation. Such information shall at the time when Personal Data is obtained, 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;
- 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 Section 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 the 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

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

13.3 INCOMPATIBILITIES WITH LOCAL LEGISLATIONS

Where an entity of the Webhelp group has reasons to believe that its local legislation prevents it from fulfilling its obligations under this Privacy Policy and has substantial effect on the guarantees provided herein, then such entity must promptly inform its Client, the Webhelp EU headquarters or the Webhelp EU member with delegated data protection responsibilities or the relevant privacy officer/function.

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

13.4 DUTY TO COOPERATE

In any event, the entities of the Webhelp group agree to cooperate with data protection authorities, including by enabling such data protection authorities to perform audits thereof, and to comply with any advice that may be provided in relation to this Privacy Policy.

Where acting as Data Processor, Webhelp commits to cooperate within a reasonable timeframe and to the extent reasonably possible with its Clients and to assist them to comply with the Applicable Data Protection Legislation.

When acting as a data controller or as a data processor, Webhelp and, where applicable, Webhelp's representative shall make available, upon request, the records of processing activities to the data protection authority only.



14. Audit

Webhelp commits to develop and integrate into its audit program the review of its compliance with this Privacy Policy. The audit program will enable Webhelp to define:

- a reasonable frequency according to which audits shall be carried out;
- the expected scope of the audit; and
- the team in charge of the audit.

The audit procedure is detailed in Appendix 7 – Procedures for Data Privacy Audits. The audit covers all significant aspects of this Privacy Policy including methods of ensuring that corrective actions will take place.

Webhelp commits to have audits conducted on a regular basis by an internal or external audit team advised by the DPO, which roadmap is initiated and determined by the DPO. The DPO is responsible for determining the scope of audits to be performed. To this end, it can consult the Privacy Data Council.

The results of each audit will be submitted to the Privacy Data Council for information. The final report, defect identification and remedial actions are to be shared and enforced by the Local Privacy Leader. Based on the Local Privacy Leader assessment, the report may be shared, where appropriate, to any Business Privacy Referent, local security manager, process / system owners, board of Webhelp parent company or any other required internal employee. Remedial actions will be defined with a prioritisation to determine a schedule for implementing such measures.

Webhelp acknowledges that competent supervisory authorities as well as Webhelp's Clients, if directly impacted by the audit, can request communication of the audit results and thus agree to grant them access thereto upon request. The results of the audit reports and relevant internal audit reports will be maintained in a form that supervisory authorities located in the EEA may access them if they utilize their audit right set out below.

If required, Webhelp entitles data protection authorities to carry out data protection audits themselves. In this respect, each Webhelp Entity shall permit the local supervisory authority to audit the relevant Webhelp Entity in order that the supervisory authority may obtain the information necessary to demonstrate Webhelp compliance with this Privacy Policy. Each such audit shall be subject to the same scope and subject to the same conditions as where the local supervisory authority audits the Webhelp Entity under the local data privacy law.

In addition, where Webhelp is acting as Data Processor, its Clients can request, on a reasonable prior notice with reasonable intervals and in any case no more than once per year, and at their own cost, that Webhelp conduct audits to assess its compliance or the compliance of its sub-processors with the Service Agreement as well as with this Privacy Policy.

In this event, Webhelp shall make available to the Client all information necessary to demonstrate compliance with Applicable Data Protection Legislation, this Privacy Policy and applicable Data Processing Agreement and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client in accordance with the Service Agreement.

Such Audit will comply with the procedure set forth in Webhelp procedures for Data Privacy Audit (Appendix 07).



15. Changes to the privacy policy

Webhelp DPO will ensure that it keeps up to date a list of entities bound by the Privacy Policy. Where any new entity of Webhelp shall be bound by the Privacy Policy, Webhelp DPO shall update the list and shall inform at least once a year or when deemed necessary by the DPO: (i) each Webhelp Entity; (ii) its employees; (iii) its Clients; and (iv) the competent data protection authorities.

To the same extent where an amendment has substantial impact on the Privacy Policy or on the level of protection of the rights granted by this Privacy Policy, Webhelp undertakes to inform in due course and on a timely manner the above-mentioned stakeholders.

The information regarding any such updates and/or amendments will be made on a timely manner so as to enable Webhelp Clients to acknowledge such updates and/or amendments and to take necessary actions where required. In particular, in the event of significant changes made to this Privacy Policy, the Clients are entitled to the rights defined under the Service Agreement for any change of the said Service Agreement.



- Appendix 01** List of Webhelp Entities bound by the Privacy Policy
- Appendix 02** Definitions for Privacy Policy and Procedures
- Appendix 03** Procedure for data protection organisation and governance
- Appendix 04** Procedure for privacy awareness and training program
- Appendix 05** Procedure for Data Subjects' requests where Webhelp acts as Data Controller
- Appendix 06** Procedure for Data Subjects' requests where Webhelp acts as Data Processor
- Appendix 07** Procedures for data privacy audit
- Appendix 08** Procedure for Personal Data Breach Notification
- Appendix 09** Procedure for Data Protection Impact Assessment
- Appendix 10** Information security policy





Think Human

Webhelp SAS
161 Rue de Courcelles
75017 Paris
France
privacy@webhelp.com