



# Webhelp

## PROCEDURE FOR HANDLING DATA SUBJECTS REQUEST - PROCESSOR

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivPro-06
Version	V3.0
Approved	25/05/2018
Effective	25/05/2018
Last version	17/01/2019
Classification	Public Viewable

Date	Version	Comments

# TABLE OF CONTENTS

<b>1. Introduction</b>	<b>3</b>
<b>2. Objectives of the procedure</b>	<b>4</b>
<b>3. Procedures</b>	<b>5</b>
3.1 <i>Request directly received by Webhelp</i>	5
3.1.1 Internal communication	5
3.1.2 Transfer of the request to the client	5
3.1.3 Webhelp assistance to the client	5
3.2 <i>Request sent by the data controller to Webhelp</i>	6
3.2.1 Internal communication	6
3.2.2 Request assesment	6
3.2.3 Answer type identification	6
3.2.3.1 Case 1	7
3.2.3.2 Case 2	7
3.2.3.3 Case 3	7
3.2.4 Escalation process	7
3.2.5 Refusal of a request	7
3.2.6 Refusal of a request	8

# 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, any regulation relating to the processing of Personal Data applicable during the term of the Privacy Policy. As a consequence, Webhelp has implemented the following procedure.

The capitalised terms used herein shall have the same meaning as specified under the Privacy Policy.



## 2. Objectives of the procedure

Data Subjects, including employees of Webhelp, are granted specific rights regarding the processing of their Personal Data as further defined under Section 7 of the Privacy Policy.

When acting as Data Processor, Webhelp shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("Requests") is addressed in a timely manner as defined hereunder, in order to comply with the Privacy Policy and Applicable Data Protection Legislation. However, this shall only apply where Webhelp actually processes the requested information.

This document describes how Webhelp shall handle a Data Subject's Request where Webhelp acts as Data Processor (stakeholders, steps and timeline). Conversely, the Requests received from Data Subjects whose Personal Data is processed by Webhelp on its own behalf only, as a Data Controller, shall be handled according to the procedure specifically defined under the Policies and **Procedure 05 - Procedures for handling Data Subjects' requests where Webhelp acts as Data Controller**

In most cases, a Request from an individual (e.g. a Client's employee, client end user) will fall within the following situation:

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

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

**As a consequence, the cost and technical impacts of the Request must be anticipated and addressed at the beginning of each engagement.**



## 3. Procedures

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

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

### 3.1 Request directly received by Webhelp

#### 3.1.1 Internal communication

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

As a matter of efficiency, such Request can also be communicated to the DPO through the following email: **Privacy@webhelp.com**

The latter will then allocate the Request to the relevant Local Privacy Leader no later than 1 working day after receipt thereof.

The information provided by the employee or workforce of Webhelp must at least specify the following information:

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

Business Privacy Referent shall immediately inform its Local Privacy Leader

#### 3.1.2 Transfer of the request to the client

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

The Local Privacy Leader will also inform the DPO that the Request has been transferred to the Client.

#### 3.1.3 Webhelp assistance to the client

At the same time, the Local Privacy Leader shall assess and verify if Webhelp actually processes the Personal Data of the Data Subject addressing the Request.

**No answer shall be provided without Client's instructions**

Should the Client allow Webhelp to handle the Request on its behalf, the Local Privacy Leader shall determine with the Client whether the Client itself or Webhelp shall acknowledge receipt of the Request and inform the Data Subject of Webhelp's role in the processing of his/her Request.

**Unless otherwise expressly instructed by the Client, Webhelp shall not enter into contact with the Data Subject during the entire procedure.**



## 3.2 Request sent by the data controller to Webhelp

### 3.2.1 Internal communication

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

Where a Client sends to Webhelp a Data Subject's Request regarding the processing of his/her Personal Data to handle, Webhelp shall acknowledge receipt thereof to the Client no later than 2 working days after receiving such Request.

No later than 5 working days after the reception of the Request, Webhelp must verify the extent to which it can address and handle the Request.

### 3.2.2 Request assesment

Upon receipt of a Request, either directly from the Data Subject or from the Client, and subject to the provisions and steps described in this Procedure, the Local Privacy Leader, or any other individual or entity, internal or external, appointed by the Local Privacy Leader for the purpose of managing the following duties shall ensure and verify that he/she has all information necessary from the Client and the Data Subject to address his/her Request, in particular:

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

Noteworthy, the gathering of such information must be limited to what is currently available within Webhelp. No additional information will be collected.

**Webhelp shall refrain as much as possible from communicating with the Data Subject even if required by the Client. Where such request is sent to Webhelp, Webhelp shall first discuss with the Client the real opportunity to have Webhelp entering directly into contact with the Data Subject. If Webhelp accepts direct contacts with the Data Subject, Webhelp must inform the Client that the latter retains the entire responsibility vis-à-vis the Data Subject for handling in due course such Request.**

### 3.2.3 Answer type identification

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

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





Three cases are then possible. These are as follow

### 3.2.3.1 Case 1

Where the information provided by the Data Subject is **not sufficient** to handle the Request, the Local Privacy Leader, or any other individual or entity, internal or external appointed by the Local Privacy Leader for the purpose of managing the following duties, shall send a request for additional information to the Client no later than 2 working days after receiving the Request.

Where the Request is too complex, and subject to compliance with any legal requirement, the timeline of the response may be extended up to 20 working days, subject to documentation of the assessment of the complexity by the Local Privacy Leader.

### 3.2.3.2 Case 2

Where the Local Privacy Leader considers on initial assessment, that the Request may **not be reasonable**, he/she shall not immediately close the case. The Local Privacy Leader, or any other individual or entity, internal or external, appointed by the Local Privacy Leader for the purpose of managing the following duties, shall reply to the Client within 10 working days after receiving the Request, by asking the Client to provide additional information as to why the Data Subject intends to exercise its rights.

Upon receipt of additional information, where the Local Privacy Leader still considers that the Request addressed by the Data Subject is not reasonable, the Local Privacy Leader shall document why it considers the Request is not reasonable and shall ensure, after approval of the DPO in writing, to reply to the Client or Data Subject, if expressly instructed by the Client, no later than 15 working days after receiving the additional information.

The response shall include the reason for not taking an action and the possibility for the Data Subject to lodge a complaint with a data protection authority and seek a judicial remedy. The wording of such response shall be validated by the DPO and the Client.

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

### 3.2.3.3 Case 3

Where information provided by the Client and/or the Data Subject is sufficient, the Local Privacy Leader shall make sure that it responds to the Request, pursuant to the instructions of the Client, within 3 weeks from the receipt thereof and duly informs in writing the DPO about the timing and content of the response so provided.

## 3.2.4 Escalation process

In the case of a complaint received directly from a Data Subject as to how its Request has been addressed, whether during or after the response has been given, the Local Privacy Leader shall ensure that it shares with the Client and the DPO the matter, no later than 3 working days after receiving the Data Subject's complaint.

For each of the above steps, and where necessary to handle the case appropriately, the Local Privacy Leader shall be ready to cooperate with the DPO by providing the latter with any relevant information in relation to the matter and inform the Client of the handling of the procedure.

The Group Data Protection Officer's guidance shall be binding. However, the DPO shall not enter into contact directly with the Data Subject, unless expressly required by the Client and the Local Privacy Leader.

## 3.2.5 Refusal of a request

Although Webhelp is committed to handling Data Subjects' Requests efficiently, under certain circumstances as defined below, Webhelp may be entitled not to accept the Client or Data Subject Request.

Webhelp can oppose the Client's or Data Subject's Request, where agreeing to the Request would imply that the following information would be shared:



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

Where there is a conflict of privacy, Personal Data may be redacted before it is shared with the Client or the Data Subject.

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

### 3.2.6 Refusal of a request

If the Client requires Webhelp to handle the Request on its behalf, the following rules shall apply when Webhelp communicates with the Data Subject.

**Under no circumstances and unless otherwise expressly instructed by the Client, shall Webhelp enter into contact with the Data Subject during the entire procedure. Even if required by the Client, Webhelp shall refrain as much as possible from communicating with the Data Subject.**

When communicating with the Data Subject, Webhelp shall cooperate with the Data Subject and address any Request in a timely manner. All communication shall be provided using clear and plain language, in an intelligible, concise, easily accessible and understandable form.

The information to be provided to Data Subjects shall be accurate and limited to (i) what the Data Subject has requested and (ii) the list of information that may be provided by a Data Controller according to the Applicable Data Protection Legislation.

**The Local Privacy Leader shall pay particular attention to the deadlines mentioned in this Procedure.**

As a general rule, Webhelp shall not apply fees for reasonable Data Subject Requests. However, under certain circumstances, in particular where the handling of the Request would imply important efforts from Webhelp, reasonable fees, subject to a national maximum according to applicable laws, may apply provided that the Data Subject is informed about such fees in advance.

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







Think Human

**Webhelp SAS**  
161 Rue de Courcelles  
75017 Paris  
France  
[privacy@webhelp.com](mailto:privacy@webhelp.com)