PROCEDURE FOR HANDLING DATA SUBJECTS REQUESTS - CONTROLLER

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivPro-04
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

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 **Procedure 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

3.1.1 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.

3.1.2 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:

3.4.1 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.

3.4.2 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.

3.4.3 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 in 2.4, 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.

Think Human

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