AUDIT PROCEDURE

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivPro-07
Version	V3.0
Approved	25/05/2018
Effective	25/05/2018
Last Version	17/02/2019
Classification	Public Viewable

Date	Version	Comments

SUMMARY

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. Policies

The Privacy Policy defines a set of principles and requirements applicable where Webhelp processes Personal Data both as Data Controller and as Data Processor. It is Webhelp's responsibility to ensure that these principles and procedures are implemented within the organization and, in particular, to verify that the Webhelp entities both commit to comply with the requirements and apply them.

Hence, for this very reason, Webhelp has decided to define an audit plan applicable to all the Webhelp entities part of the group.

This data privacy audit policy and procedures shall also apply to external audits which Webhelp may need to conduct to monitor third parties compliance with applicable terms of the contracts with which they are bound. In addition, it has to be noted that where Webhelp acts as Data Processor it may be requested by its Clients to conducts specific audits. The conditions of such audit should be defined by Webhelp and the Client in the agreement they enter into.

3. Procedures

The purpose of data protection audits (hereinafter the Audits) is to provide the Group Data Protection Officer (“DPO”), the Privacy and Data Council, the persons being the main point of contact of the DPO and dealing with data protection matters within each Webhelp Entity. ("Local Privacy Leaders") and the board of Webhelp parent company with an overview of the level of compliance of Webhelp regarding the Privacy Policy and the applicable data protection legislation.

Where Audits demonstrate that one or several Webhelp entities do not comply with the Privacy Policy and/or with the Applicable Data Protection Legislation, the DPO, the Data Privacy Council and the board of Webhelp parent company shall define a remediation plan to ensure that the points of non-compliance are remediated.

3.1 Scope of Data Privacy Audit

3.1.1 Scope of Data Privacy Audit

Webhelp commits to audit on a regular basis (as provided below) the processing of Personal Data relating to its employees, agency staff, sub-contractors, suppliers and Clients or any other processing of Personal Data.

3.1.2 Material scope of Data Privacy audit

Scope of the Data Privacy Audit may cover the compliance with any applicable law or regulation and/or any of the following documents can be reviewed:

- the existing Privacy Policy;
- the procedures in place to ensure that the Privacy Policy is implemented;
- the register in place;
- the data transfers agreement in place;
- agreements with Webhelp’s Clients;

Therefore, Scope of the Data Privacy Audit may include all or part of the following areas:

i) Compliance with the governance as defined in the Privacy Policy

- roles and responsibilities;
- policies & standards;
- derogations / exceptions to the Privacy Policy *as per* applicable local law;
- enterprise security / privacy risk assessments;
- training and awareness;
- compliance with clients’ and third parties’ contractual agreements;
- monitor new privacy laws and regulations;

ii) Compliance of the processing in place

- records of data processing;
- records of the transfer mechanism used for cross-border data flows;
- legal and physical mechanisms for data transfer;
- lawfulness of the purposes of processing;
- legal basis for the processing (to also include alignment with all purposes of processing);
- data protection / privacy impact assessments (DPIA / PIA);
- data retention requirements;

iii) Privacy by design and accountability

- address privacy obligations (e.g. Privacy by Design) and rights (e.g. response to privacy requests and complaints);
- proportionality of the Personal Data processed;
- application of the data retention requirements;
- transparency, information provided to the Data Subjects;
- Data Subject consent management;

- logical and physical security measures in place for the protection of the data at rest / in transit;
- technical facilities storing personal data (e.g. data centre, servers, SaaS IT tool)
- privacy breach response and reporting; and/or
- self-assessments of privacy compliance.

3.1.3 Determination of the scope of Data Privacy Audit

The DPO is responsible for determining the scope of Audits to be performed in cooperation with internal or external accredited audit teams. To this end, the Privacy Data Council can be consulted.

The DPO can decide that Audits be targeted:

- Locally (i.e. covering specific countries, business line or specific data processing);
- Per project/application; and/or
- Per function (e.g. HR, marketing, etc.).

The DPO shall advise on the precise scope of a given Audit before it starts and may further expressly define it in the mission order as defined below.

Audits will be supervised by the DPO, supported by Local Privacy Leaders and internal audit teams belonging to the Data Privacy Council or external audit teams, as may be required.

Webhelp commits to audit the processing of its employees' and Clients' Personal Data that it processes on its own behalf but also the processing which it conducts on behalf of its Clients. As mentioned above, in the latter case, the conditions of the Audit shall be defined and agreed by Webhelp and the Client in the contractual agreement they have entered into.

3.1.4 Instigation of Data Privacy Audit

Audits can be instigated:

- as unscheduled and/or scheduled Audits by the DPO regarding either some specific processing or for the implementation of the Data Privacy Policy;
- by the Privacy Data Council regarding the governance and compliance with the Webhelp Data Privacy Policy
- at the request of the executive management (e.g., following an incident of concern); and/or
- by a Client or a competent authority which would be subject to the requirements of an external body.

3.1.5. Frequency of Data Privacy Audit

Webhelp shall conduct Data Privacy Audits:

- On the spot Audits, at least once a year;
- Scheduled Audit of general compliance for limited geographies and/or entities and/or functions at least once a year;
- Scheduled global Audit regarding the general compliance of Webhelp with the Data Privacy Policy at least every two years.

Webhelp may decide to launch Audits where it has received a complaint from a Data Subject or further to the launch of a new project or when deemed necessary for business and compliance purposes

3.2 Methodology of Data Privacy Audit

3.2.1 Mission order

Where Webhelp has decided to launch an Audit, the following information shall be documented in a mission order prepared by the DPO and/or the internal team and/or an external auditor (the "Auditor") prior to launching such Audit:

- scope of the Audit (material and geographical);

- functions and persons to be interviewed;
- period of Audit;
- documentation to be reviewed.

The mission order shall be communicated to the interviewed persons before the Audit starts and at the latest at the beginning of the interview.

3.2.2 Audit notification

The mission order shall be communicated by the Auditor to the auditees and appropriate leadership, Local Privacy Leader before the Audit begins and at the latest at the beginning of the first interview. Purposefully, no minimum notice period is mandated.

3.2.3 Audit phase

During the Audit phase, the Auditor shall collect sufficient information to draw relevant conclusions.

The Audit can take the following forms:

- questionnaires;
- documentation / computerized systems review;
- floor inspection;
- interview; or
- a combination of the above.

As part of the Audits, the Auditor may need to visit key departments and sites relevant regarding the scope of the Audits as expressly defined.

Audits can take place in particular through documentation review and interviews.

3.3 Consequence of Data Privacy Audit

3.3.1 Audit conclusion

Based on the information collected, an Audit report shall be drafted. Each Audit report shall be organised around the following structure:

- Presentation of the scope of the Audit;
- Presentation of the documents reviewed and/or of the persons interviewed;
- Description of the processing and/or of the procedures audited;
- Conclusion regarding the level of compliance of the processing and/or of the procedure audited;
- Remediation measures with prioritisation of the measures;
- Roadmap to ensure that the remediation measures are effectively implemented.

First Audit report, irrespective of the scope of the Audit shall be drafted by the Auditor, reviewed by the DPO and submitted to the Privacy Data Council and to the board of Webhelp parent company, if necessary, for information.

Unless otherwise agreed, Audit reports are confidential and shall follow disclosure rules attached to confidential and internal documents.

Final report shall be reviewed by the Local Privacy Leader. Once the report, defects and remedial actions are agreed with the auditees the final Audit report shall be distributed by the Local Privacy Leader for local application and shared with all permanent and non-permanent members of the Privacy and Data Council, to the board of Webhelp parent company and to the board of the local Webhelp Entity.

As a consequence, the final Audit report shall be shared, based on the Local Privacy Leader assessment, to any of the following individual:

- Business Privacy Referent
- Local security manager
- Process / system owners;
- Board of Webhelp parent company;
- Any other required internal employee

In the event of disagreement on the findings and/or actions resulting from the Audit the DPO shall be the final arbitrator

3.3.2 Audit follow-up

Once the remediation measures and roadmap are defined, the DPO shall make sure that the measures are effectively implemented. Implementation shall be conducted and monitored by the Local Privacy Leader. A report shall be produced by the implementation team, half way between the beginning of the remediation plan and the scheduled end of implementation in order to monitor the implementation of the remediation measures.

If any adaptation to the agreed remedial actions is required, the Local Privacy Leader and the DPO will submit the agreed updated remediation measures and roadmap to the Privacy and Data Council for information.

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