PROCEDURE FOR DATA PROTECTION IMPACT ASSESSMENT

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivPro-09
Version	V3.0
Approved	25/05/2018
Effective	25/05/2018
Last Version	17/01/2019
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. Objectives of the procedure

The Data Protection Impact Assessment (“DPIA”) is a Risk-based process introduced by the General Data Protection Regulation - European Regulation 2016/679 - (“GDPR”) that enables the controller to describe the Data Processing, to prove its necessity and proportionality and help manage the Risks to the rights and freedoms of natural persons resulting from the processing of personal data4 by assessing them and determining the measures to address them

It is also a way for Webhelp to demonstrate that necessary Procedures are implemented within its organisation in order to comply with any Applicable Data Protection Legislation and the accountability principles. DPIA is a process for building and demonstrating compliance and anticipate Risk attached to Data Processing.

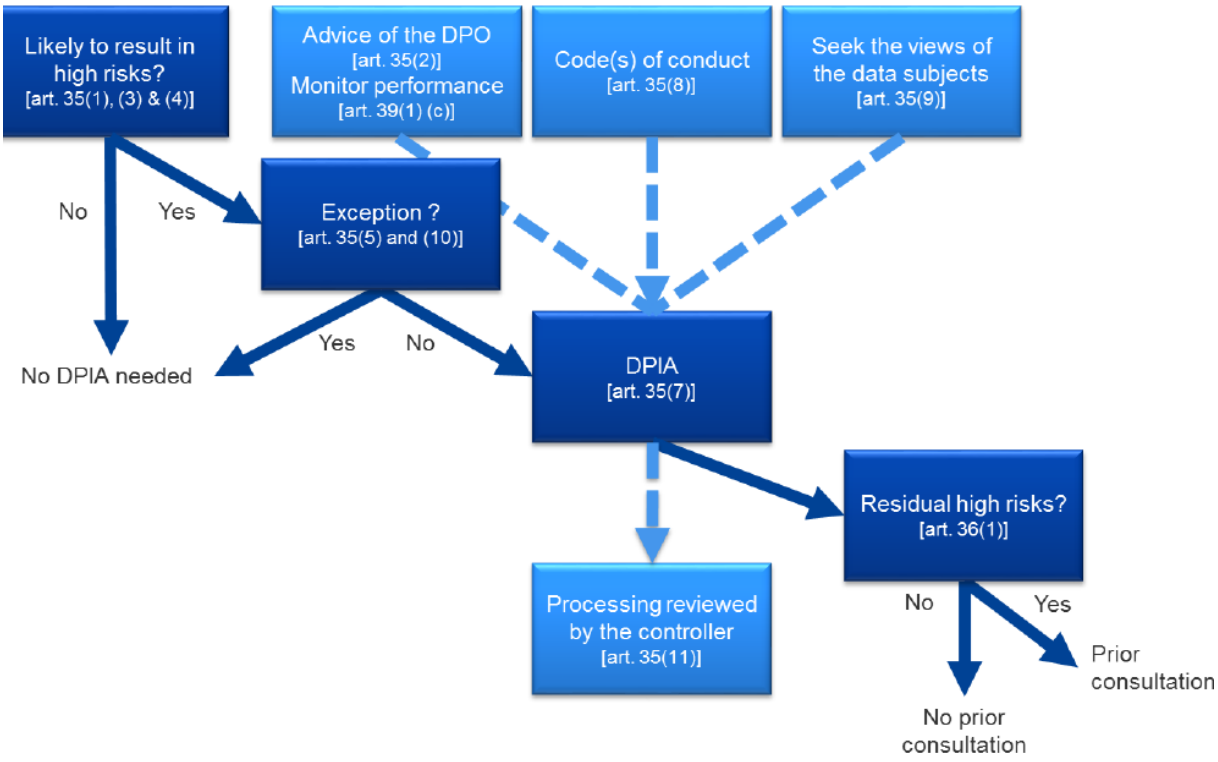
Therefore, a DPIA aims at “managing risks” to the rights and freedoms of natural persons, using the following processes, by:

- establishing the context: “taking into account the nature, scope, context and purposes of the processing and the sources of the risk”;
- assessing the risks: “assess the particular likelihood and severity of the high risk”;
- treating the risks: “mitigating that risk” and “ensuring the protection of personal data”.

3. Procedures

In line with the Risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "likely to result in a high Risk to the rights and freedoms of natural persons".

The following procedure can be described as follow:



Webhelp is committed to preserving Data Subjects from any Risks to their rights and freedoms. Such Risk shall include, but are not limited to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

3.1 DPIA Obligation when Webhelp is acting as Data Processor

If the processing is wholly or partly performed by Webhelp as a Data Processor, **Webhelp should assist the Data Controller** in carrying out the DPIA and provide any necessary information in accordance with any applicable Data Protection Legislation and/or contractual obligation.

The Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the Data Controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the Risk assessment and whether the residual Risk is acceptable, and to develop knowledge specific to the Data Controller context;

The Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the Data Controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

3.2 DPIA Obligation when Webhelp is acting as Data Controller

3.2.1 Criteria to determine if a DPIA is mandatory

Although there is no exhaustive list of situations in which a DPIA should be proceeded, Webhelp is committed to apply a consistent approach in which a DPIA is mandatory. Furthermore, it is widely considered within Webhelp that such circumstances where it is not clear whether a DPIA is required, a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law. Illustration are provided in Working Document 1.

3.2.1.1 Identification of the Processing and the Risks requiring DPIA to be processed.

3.2.1.1.1 Principles

Where a type of processing, in particular using new technologies, is likely to result in a **high Risk** to the rights and freedoms of natural persons, Webhelp shall, prior to the processing, carry out DPIA.

Shall be considered as processing that are likely to result in high risks:

- A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. Such situation could be met when analysing or predicting aspects concerning
- Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences; or
- A systematic monitoring of a publicly accessible area on a large scale.

The requirement of this procedure applies to existing Processing operations

3.2.1.1.2 Criteria

Webhelp acknowledges, that in accordance with Applicable Data Protection Legislation, some Data Processing as Data Controller or as a Data Processor, may require a DPIA. Therefore, Webhelp is committed, when acting as a Data Controller, top implement a DPIA if the following criteria is met and the Data Processing is likely to result in a high risk.

- **Evaluation or scoring**: including profiling and predicting, especially from aspect concerning performance at work, economic situation, health, personal preferences of interests, reliability or behaviour, location or movement.
- **Automated-decision making with legal or similar significant effect**: processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person” (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion
- **Systematic monitoring**: processing used to observe, monitor or control Data Subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).
- **Sensitive Data or Data of a highly personal nature**: This includes household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement, personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging application, financial data, Bank or payment information that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes.
- **Data processed on a large scale**: This criterion shall be assessed based on the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data

and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity.

- **Matching or combining datasets**: For example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the Data Subject
- **Data concerning vulnerable data subjects**: Vulnerable data subjects may include children employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified
- **Innovative use or applying new technological or organisational solutions**, like combining use of finger print and face recognition for improved physical access control, etc. It is clear that the use of a new technology, defined in "*accordance with the achieved state of technological knowledge*" (recital 91), can trigger the need to carry out a DPIA.
- **When Data processing include any activity covered by Webhelp Code of Conduct**
- When the processing in itself "**prevent Data Subjects from exercising a right or using a service or a contract**". This includes processing operations that aims at allowing, modifying or refusing Data Subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.
- The Data is intended to be processed for a purpose other than that for which the personal data were collected

3.2.1.2 Identification of the Processing and the Risks where DPIA is not mandatory

Webhelp does not consider that a DPIA is required in the following cases:

- Where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons;
- When the nature, scope, context and purposes of the Processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used;
- When the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed;
- Where a processing operation is necessary for compliance with a legal obligation to which Webhelp is subject except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities; and,
- Where the processing is included on the optional list (established by the Supervisory Authority) of processing operations for which no DPIA is required and if the processing falls strictly within the scope of the relevant procedure mentioned in the list.

It is widely considered within Webhelp that such exception shall be strictly interpreted.

3.2.2 Conducting a DPIA

3.2.2.1 When to carry out a DPIA

DPIA should be carried out "prior to processing". A DPIA should be conducted as early as is practicable as part of the design of the processing operation, even if some of the processing operations are still unknown. This is consistent with data protection "by design" and "by default" principles. DPIA shall be updated during the product or service development.

The DPIA should be seen as a tool for helping decision-making concerning the Processing and **carrying out a DPIA is a continual process, not a one-time exercise.**

3.2.2.2 Who should carry out the DPIA

The DPIA shall be carried by the Information Owner, product manager, specific business units, User etc.

Webhelp's Data Protection Officer (DPO), shall give advice about the DPIA procedures implemented within the organisation.

The Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the Data Controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the Risk assessment and whether the residual Risk is acceptable, and to develop knowledge specific to the Data Controller context;

the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the Data Controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs

Notwithstanding the above, liability and responsibility may lay at the Data Controller.

3.2.2.3 Applicable Methodology to carry out the DPIA

A DPIA should include at a minimum the following items:

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing;
- An assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to:
    - address the risks;
    - Demonstrate compliance with this Regulation".

Compliance with a Code of Conduct Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by Data Controller controllers and Data Processor as well as Binding Corporate Rules (BCR), should be taken into account. Any applicable methodology to carry out a DPIA shall comply with the minimum set of criteria determine in Working Document 2

3.3 Prior Consultation

Where a DPIA reveals high residual risks, Webhelp will be required to seek prior consultation for the processing from the Supervisory Authority (Article 36(1)). When consulting the Supervisory Authority Webhelp shall provide the Supervisory

Authority with:

- Where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- The purposes and means of the intended processing;
- The measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
- The contact details of the data protection officer
- The conducted DPIA; and,
- Any other information requested by the supervisory authority.

The Supervisory Authority may provide its advice in accordance with the Applicable Data Protection Legislation and shall not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents. It is underlined that the Supervisory Authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, That period may be extended by six weeks. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

For the avoidance of doubt, the Processing shall not be processed until the consultation of the Supervisory Authority has been fully conducted.

3.4 Role of the DPO

DPO may designate any other individual or entity, internal or external, for the purpose of managing the duties attached to any section of this Procedure.

DPO shall be consulted when a DPIA is conducted in order to assess the compliance of the Data Processing with any Applicable Data Protection Legislation and any internal Rules, Code etc. The DPO should also monitor the performance of the DPIA. Furthermore, any DPIA methodology developed within Webhelp shall be approved by the DPO in order to ensure compliance with the criteria determine in Working Document 2

As a matter of good practice and under the DPO audit program as described in Procedure for Data Privacy Audits DPIA should be continuously reviewed and regularly re-assessed.

3.5 Documentation and record keeping

Therefore, in addition, of the above, the DPO shall document any decision related to any DPIA in order to enable the Supervisory Authority to verify compliance with any Applicable Data Protection Legislation. Shall be adequately recorded:

- The reasons for not carrying out a DPIA, and include/record the views of the data protection officer.
- Document any DPIA conducted within its Data Processing Register and include in such documentation, the purposes of processing, a description of the categories of data and recipients of the data and “where possible, a general description of the technical and organisational security measures” and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

When DPO has designated any other individual or entity, internal or external, for the purpose of managing the duties attached to any section of this Procedure, DPO shall be (1) informed of any DPIA conducted and (2) receive all above documentation in a timely manner.

Publishing a DPIA is not a legal requirement but, with the Data Controller approval, all or part of a DPIA could be communicated to any third Party if required. The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA’s main findings, or even just a statement that a DPIA has been carried out.

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.

Working Document 1

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA

Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A hospital processing its patients' genetic and health data (hospital information system).	Sensitive data or data of a highly personal nature. Data concerning vulnerable data subjects. Data processed on a large-scale.	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	Systematic monitoring. Innovative use or applying technological or organisational solutions.	Yes
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	Systematic monitoring. Data concerning vulnerable data subjects.	Yes
The gathering of public social media data for generating profiles.	Evaluation or scoring. Data processed on a large scale. Matching or combining of datasets. Sensitive data or data of a highly personal nature:	Yes
An institution creating a national level credit rating or fraud database.	Evaluation or scoring. Automated decision making with legal or similar significant effect. Prevents data subject from exercising a right or using a service or a contract. Sensitive data or data of a highly personal nature:	Yes
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials	Sensitive data. Data concerning vulnerable data subjects. Prevents data subjects from exercising a right or using a service or a contract.	Yes
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91).	Sensitive data or data of a highly personal nature. Data concerning vulnerable data subjects.	No
An online magazine using a mailing list to send a generic daily digest to its subscribers.	Data processed on a large scale.	No
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	Evaluation or scoring.	No

Working Document 2

Criteria for an acceptable DPIA

DPIA includes as systematic description of the processing is provided:

- Nature, scope, context and purposes of the processing are taken into account;
- Personal data, recipients and period for which the personal data will be stored are recorded;
- A functional description of the processing operation is provided;
- A the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
- A compliance with approved codes of conduct is taken into account;

DPIA includes an assessment of the necessity and proportionality of the Processing:

- Measures envisaged to comply with the Regulation are determined taking into account:
    - Measures contributing to the proportionality and the necessity of the processing on the basis of:
        - Specified, explicit and legitimate purpose(s);
        - Lawfulness of Processing;
        - Adequate, relevant and limited to what is necessary data;
        - Limited storage duration (Article 5(1)(e));
    - Measures contributing to the rights of the data subjects:
    - Information provided to the data subject;
    - Right of access and to data portability;
    - Right to rectification and to erasure;
    - Right to object and to restriction of processing;
    - Relationships with processors ;
    - Safeguards surrounding international transfer(s);
    - Prior consultation.

DPIA explains how Risks to the rights and freedoms of data subjects are managed:

- Origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
- Risks sources are taken into account;
- Potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
- Threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
- Likelihood and severity are estimated;

- Measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

DPIA as involved interested parties:

- The advice of the DPO is sought;
- The views of data subjects or their representatives are sought, where appropriate.

Think Human

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