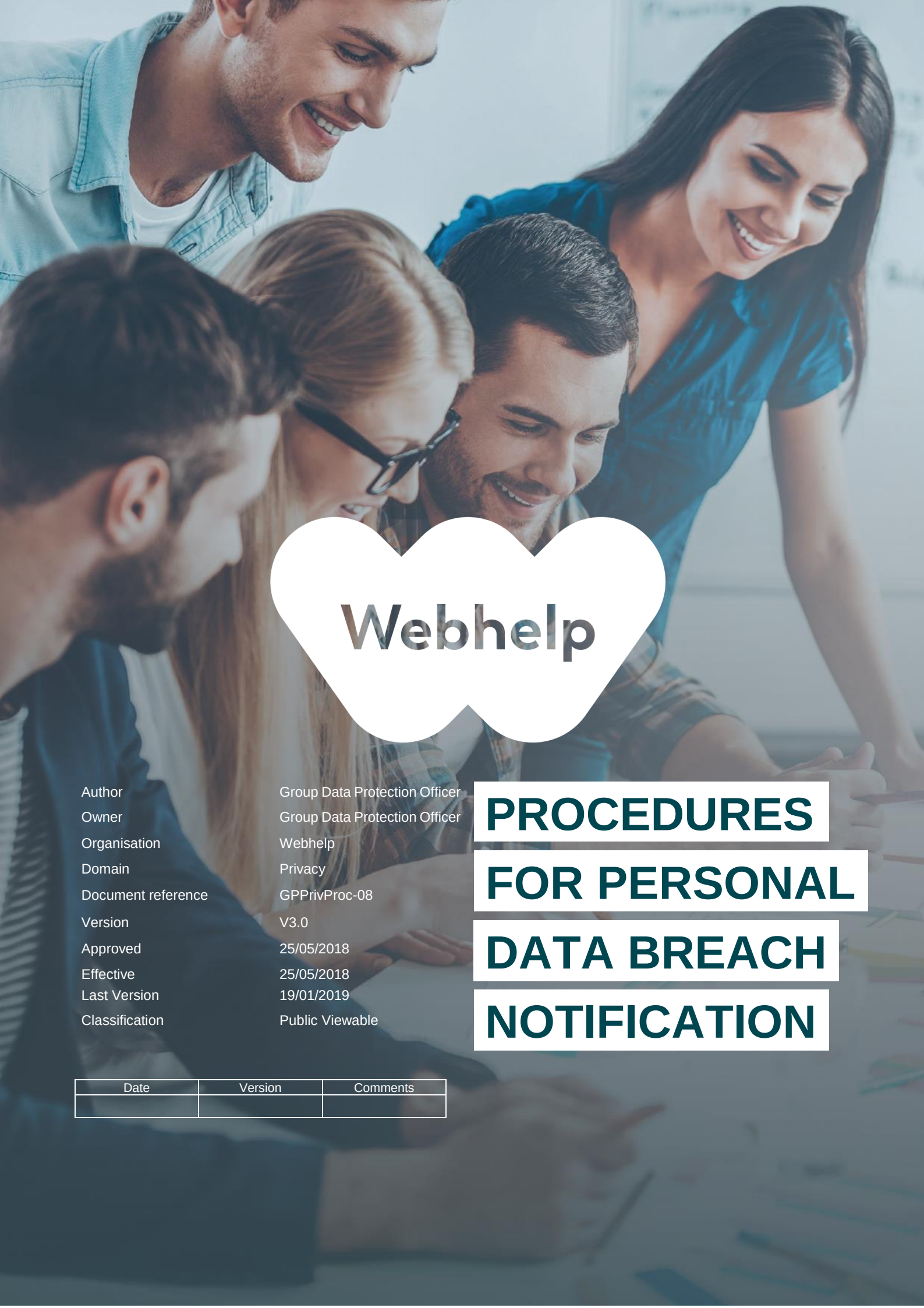

PROCEDURES FOR PERSONAL DATA BREACH NOTIFICATION

Author	Group Data Protection Officer
Owner	Group Data Protection Officer
Organisation	Webhelp
Domain	Privacy
Document reference	GPPrivProc-08
Version	V3.0
Approved	25/05/2018
Effective	25/05/2018
Last Version	19/01/2019
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, 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 General Data Protection Regulation (the GDPR) introduces the requirement for a Personal Data Breach to be notified to the competent national supervisory authority and, in certain cases, communicate the breach to the individuals whose personal data have been affected by the breach. Such obligation shall not apply if the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals

In order to detect and promptly contain a Personal Data Breach, anticipate the consequences of a Personal Data Breach, and to mitigate the risk to the rights and freedoms of individuals, Webhelp has implemented technical and organisational measures based on a “risk approach” and further described through its:

- Information Security Policy
- Data classification and categorisation policy
- Data Protection Impact Privacy Procedure.

Such measures allow Webhelp to (1) Implement an appropriate level of security attached to the Processing of Personal Data; and (2) Effectively address in an appropriate and timely manner any Personal Data Breach. A Personal Data Breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons. This can include loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

When acting as a Data Controller or as a Data Processor, Webhelp shall through the Personal Data Breach Notification procedure focus on protecting individuals’ personal data when assessing a possible Personal Data Breach.

3. Definition and scope

The General Data Protection Regulation defines a "**Personal Data Breach**" as;

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The following terms shall be construed and understood as:

DESTRUCTION	Means where the data no longer exists, or no longer exists in a form that is of any use to the Data Controller.
DAMAGE	Means where personal data has been altered, corrupted, or is no longer complete.
LOSS	Means a situation where the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.
UNAUTHORISED OR UNLAWFUL PROCESSING	Means the disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

Webhelp Group Information Security Policy ("**Webhelp Information Security Policy**") defines a "**Security Incident**" as an :

"Attempted or successful unauthorised access, use, disclosure, modification, or destruction of Information or interference with system operations in the Information System.

In accordance with the Webhelp Information Security Policy, a Personal Data Breach shall always be considered as a Security Incident involving Personal Data.

It shall be underlined that all Personal Data Breaches are Security Incidents, but all Security Incidents are **not** Personal Data Breaches.

3.1 INTERNAL ASSESSMENT RELATED TO POTENTIAL PERSONAL DATA BREACH

3.1.1 PRINCIPLE

As all Personal Data Breaches are a Security Incident, this Personal Data Breach Notification Procedure shall be applied in addition to any applicable Information Security policy and procedure and the following provisions shall apply, if Personal Data forms part of the potential Breach:

"All Security Incidents and suspected weaknesses shall be reported to the CISO via the locally documented procedures in order to allow Webhelp to: (1) identify and respond to suspected or known Security Incidents; (2)mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Webhelp; and (3) document Security Incidents and their outcomes (4) All information Security Incidents shall be investigated to establish their cause and impacts with a view to avoiding similar events.

Reporting of Security Incidents shall follow the applicable rules attached to the Webhelp Information Security Policy and locally documented procedures. The former shall prevail in case of discrepancy.

Such procedure shall include report upwards systems in order to address the appropriate level of management and determine who has operational responsibility within the organisation for managing a Security Incident and how or whether to escalate a Security Incident in a timely manner and with no undue delay. The Webhelp Chief Information Security Officer ("CISO") shall implement and document the implementation of adequate training with regards to Security standards. Such training shall be provided to all users of Webhelp Information Systems and shall include relevant information on the existence of, procedure to disclose and how to properly react to such Security Incident.

Furthermore, under the Applicable Privacy Law, any subcontractor processing Personal Data on behalf of Webhelp shall be bound by a Contract or any other legal act under European Union or Member State law. This document shall be binding on the processor with regard to Data Protection and shall include an obligation for the subcontractor to assist Webhelp in ensuring compliance with this Procedure and or a related Security Incident.

3.1.2 DETECTION OF POTENTIAL PERSONAL DATA BREACH

Under the Webhelp Security Policy, Webhelp has implemented internal processes to detect and address a Security Incident.

3.1.2.1 DETECTION OF SECURITY INCIDENT

Webhelp shall implement appropriate technological protection and organisational measures to establish immediately whether a Personal Data Breach has taken place. In accordance with Webhelp Security Policy, 7.15 – Monitoring System access and use:

(…) Webhelp permits monitoring and recording of User activities while using Information Systems or Devices (including Data such as telephone communications and email) for the following reasons: (1) Establishing the existence of facts ; (2) Investigating or detecting unauthorised use of Information System or Device; (3) Preventing or detecting crime (…)

Such Organisational measures shall ensure that any subcontractor Processing Personal Data on behalf of Webhelp shall be bound by a Contract or any other legal act under Union or Member State law. This document shall be binding on the processor with regard to the controller and shall include an obligation for the subcontractor to assist Webhelp in ensuring compliance with this Procedure towards Webhelp and Webhelp's Data controllers.

3.1.2.2 ASSESSING POTENTIAL PERSONAL DATA BREACH

This brief period allows for further investigation, to gather evidence and to assess risk before the Data Controller may have to notify. Emphasis should be on prompt action to investigate a Security Incident to determine whether personal data have indeed been breached.

3.1.3 INTERNAL NOTIFICATION OF PERSONAL DATA BREACH TO THE DPO

CISO shall report to the DPO each Security Incident involving Personal Data when CISO has a reasonable degree of certainty that a Security Incident has occurred that has led to personal data being compromised. Such internal notification shall comply with the following:

- An email to the DPO on the dedicated email address – Privacy@webhelp.com
- As title to the email underlining the purpose the email such as Breach - Privacy
- A short summary of the available information attached to the Data Privacy Breach including where possible but not limited to
    - the nature of the Personal Data Breach
    - the categories and approximate number of data subjects concerned
    - the categories of personal data records concerned
    - approximate number of personal data records concerned;
    - the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. Approximations are allowed to be made in the number of individuals affected and the number of personal data records concerned. **The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.**

3.1.3.1 NATURE OF THE PERSONAL DATA BREACH

Nature of the Personal Breach shall be determined within one or more of the following principle

CONFIDENTIALITY BREACH	Means an unauthorised or accidental disclosure of, or access to, Personal Data.
AVAILABILITY BREACH	Means an accidental or unauthorised or temporary loss of access to, or destruction of, Personal Data.
INTEGRITY BREACH	Means an unauthorised or accidental alteration of Personal Data.

3.1.3.2 CATEGORIES AND APPROXIMATE NUMBER OF DATA SUBJECTS CONCERNED

Such information refers to the various types of individuals whose personal data has been affected by a breach. This could include:

- children and other vulnerable groups;
- people with disabilities, employees or customers;
- Webhelp Employees;
- Webhelp Sub-contractor employees;
- Webhelp customers and prospects;
- Data Controller or Client employees;
- Data Controller or Client Sub-contractor employees;
- Data Controller or Client customers and prospects; or,
- Other,

3.1.3.3 CATEGORIES AND APPROXIMATE NUMBER OF PERSONAL DATA RECORDS CONCERNED;

Such information refers to the different types of records that Webhelp may process, such as data included within the following Working Document 1.

3.1.3.4 NUMBER OF PERSONAL DATA RECORDS CONCERNED

When the number of Personal Data Records concerned by the Personal Data Breach is not available, CISO organisation may provide the DPO an approximate number of individuals affected and the number of Personal Data Records concerned.

3.1.3.5 MEASURES TAKEN OR PROPOSED TO BE TAKEN

Webhelp's primary actions will be focussed towards preventing any further access or disclosure of Personal Data. In certain circumstances, and in agreement with the DPO or relevant authorities, access may be continued to assist in identifying the source of the breach.

3.2 NOTIFICATION OF PERSONAL DATA BREACH TO THE DATA CONTROLLER WHEN WEBHELP IS A DATA PROCESSOR.

When acting as a Data Processor Webhelp will notify the Data Controller without undue delay of such Personal Data Breach. This means Webhelp will immediately notify the Data controller once the CISO has a reasonable degree of certainty that a Security Incident has occurred that has led to Personal Data being compromised. Further information about the Personal Data Breach shall be provided in phases as information becomes available.

Unless otherwise agreed, Webhelp shall not make notification on behalf of the Data Controller

3.3 PERSONAL DATA BREACH WHEN WEBHELP IS A DATA CONTROLLER.

3.3.1 PERSONAL DATA BREACH ASSESSMENT

3.3.1.1 PRINCIPLES

Based on the information provided by the CISO within the internal notification of Data Privacy Breach to the DPO, the DPO shall assess what is the appropriate notification and action to be taken by Webhelp. Immediately upon becoming aware of a breach, Webhelp shall seek to **contain the Security Incident** and **assess the risk to right and freedoms of individuals that could result from it.**

Such assessment shall determine if the Personal Data Breach is likely to result in a **high risk** (e.g if Personal Data Breach may certainly lead to physical, material or non-material damage for the individuals whose data have been breached). Such high risk Is likely to occur when Sensitive – Special categories is subject of the Breach of Personal Data. Working Document 2 of this procedure provides some useful examples of different types of breaches involving risk or high risk to individuals.

The Assessment shall be conducted by the DPO when Webhelp is acting as the Data Controller. When acting as a Data Processor, Webhelp may be required by the Data Controller to provide such assessment or to assist the Data Controller for such purpose.

3.3.1.2 FACTORS TO CONSIDER WHEN ASSESSING RISK

The following factors shall be assessed by the DPO, based on the information provided by the CISO

- The type of breach
- The nature, sensitivity, and volume of personal data -
- Ease of identification of individuals (directly or indirectly)
- Severity of consequences for individuals.
- Special characteristics of the individual
- The number of affected individuals
- Special characteristics of the data controller
- General points

3.3.1.3 CONCLUSION OF THE INTERNAL ASSESSMENT

Each assessment shall be documented in accordance with this procedure and, if deemed necessary by the DPO, disclosed to the Privacy and Data Council. Notwithstanding the above, DPO shall determine without undue delay what are next step and actions in consideration of the result of his assessment. Methodology of assessing the severity of a Personal Data Breach may be determined by the Data Controller.

Notification and communication is not necessary in all circumstances. Exceptions are outlined below:

- Notification to the competent supervisory authority is only triggered where a breach is likely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

3.3.2 NOTIFICATION TO THE SUPERVISORY AUTHORITY

As the main purpose of notification is limiting damage to Data Subjects, Webhelp is committed to have an interpretation of its obligation of notification in such a way that collaboration with the authority are to be encouraged

3.3.2.1 CONDITIONS WHERE NOTIFICATION IS NOT REQUIRED

Where a Personal Data Breach is "*unlikely to result in a risk to the rights and freedoms of natural persons*", notification to the supervisory authority is not required. Such situations may occur if Personal Data has been made essentially unintelligible to unauthorised parties (i.e securely and properly encrypted) and where the data is a copy, or a backup exists.

The above exception shall be strictly interpreted and Notification shall, unless the above are met and documented, occur within 72 hours.

3.3.2.2 TIME-FRAME

Following the assessment by the DPO, notification to the Supervisory Authority may be required. Notification to the competent supervisory authority is only triggered where a breach is likely to result in a risk to the rights and freedoms of individuals.

Once the DPO is notified by the CISO, Webhelp, if acting as a Data Controller should notify the Personal Data Breach to the Supervisory Authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

3.3.2.3 DETERMINATION OF THE SUPERVISORY AUTHORITY.

Webhelp has determined the French Authority "CNIL" as its Lead Supervisory Authority. Therefore, a Breach of Personal Data shall be notified to Webhelp's Lead Supervisory Authority.

In addition to the above, Webhelp may proactively also report an incident to one or more Supervisory Authority which is not its Lead Supervisory Authority if Webhelp is aware that Data Subjects in one or more other Member State are affected by the Personal Data Breach.

3.3.2.4 DELAYED NOTIFICATION

In certain circumstances, the DPO may require notification to the Supervisory Authority or Data Subject to be delayed when:

- Depending on the circumstances, it may take the Data Controller some time to establish the extent of the Personal Data Breaches and, rather than notify each Personal Data Breach individually, Webhelp instead organises a meaningful notification that represents several very similar Personal Data Breaches, with possible different causes.
- There are legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a Personal Data Breach.

The above exception shall be strictly interpreted and Notification shall, unless the above are met and documented, occur within 72 hours.

3.3.2.5 NOTIFICATION TO THE SUPERVISORY AUTHORITY

Notification to the Supervisory Authority shall include the following information:

- The nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
- The name and contact details of the DPO or other contact point where more information can be obtained;
- The likely consequences of the Personal Data Breach;
- 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.

All relevant and available information gathered by the DPO and the CISO within their internal notification and assessment, shall be communicated to the Supervisory Authority.

Where precise information is not available this should not be a barrier to timely Personal Data Breach notification and where, it is not possible to provide the information at the same time, the information may be provided in various phases to avoid undue delay. The Supervisory Authority should agree how and when additional information should be provided and Webhelp shall, if deemed necessary, continue its investigations.

3.3.3 COLLABORATION WITH SUPERVISORY AUTHORITY

The DPO or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing one or more Personal Data Breach(es) shall be the single point of contact of the Supervisory Authority and shall collaborate as much as possible with such Supervisory Authority.

After making an initial notification, Webhelp will update the Supervisory Authority if a follow-up investigation uncovers evidence that the Security Incident was contained and no Personal Data Breach actually occurred. This information shall then be added to the information already given to the Supervisory Authority and the Security Incident recorded accordingly as a non-breach.

3.3.4 COMMUNICATION TO THE DATA SUBJECT

When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. Communication to Data Subjects shall be done in addition to the notification of the Supervisory Authority.

3.3.4.1 CONDITIONS WHERE COMMUNICATION TO THE DATA SUBJECT IS NOT REQUIRED

The following circumstances do not require notification to Data Subjects in the event of a Personal Data Breach.

- Webhelp has applied appropriate technical and organisational measures to protect Personal Data prior to the Personal Data Breach, in particular those measures that render Personal Data unintelligible to any person who is not authorised to access it. This could, for example, include protecting Personal Data with state-of-the-art encryption.
- Immediately following a Personal Data Breach, Webhelp has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.
- For example, depending on the circumstances of the case, Webhelp may have immediately identified and taken action against the individual who has accessed Personal Data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.

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

3.3.4.2 CONTACTING THE DATA SUBJECT

Any Personal Data Breach resulting in a high risk to the rights and freedoms of natural persons should be communicated to the affected Data Subjects directly by the Data Controller or any other individual or entity, internal or external, appointed by the Data Controller for the purpose of communication to the affected Data Subjects.

Unless such direct communication would involve a disproportionate effort (ie. where their contact details have been lost as a result of the breach or are not known in the first place), an adequate notification may be to use one or more public dedicated communication means. This communication should be clear and transparent.

Transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a Personal Data Breach to an individual. Communication shall be done in one or more language.

3.3.4.3 INFORMATION TO BE COMMUNICATED TO THE DATA SUBJECT

The communication should be clear and transparent (in plain language) and describe:

- The nature of the Personal Data Breach;
- The name and contact details of the DPO or other contact point;
- An understandable description of the likely consequences of the breach;
- An understandable description of the measures taken by Webhelp to address the Breach if such measure have been taken; and,
- A set of understandable recommendations for Data Subject concerned to mitigate potential or existing adverse effects.

3.3.4.4 COLLABORATION WITH THE SUPERVISORY AUTHORITY AND AUTHORITIES

The DPO or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing one or more Personal Breach shall be the single point of Contact to the Supervisory Authority and shall collaborate as much as possible with such Supervisory Authority.

Communications to Data Subjects should be made as soon as reasonably possible and in close cooperation with the Supervisory Authority. Such communication may be done within advisable or mandatory guidance provided by the Supervisory Authority or other relevant authorities.

Webhelp will update the Supervisory Authority if (1) a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred (2) any action is taken in accordance to the above.

3.4 ROLE OF THE DPO

In consideration of the size of the Webhelp organisation and in consideration of the importance of an adequate, effective and quick action, the DPO may appoint any other individual or entity, internal or external, for the purpose of managing one or more of the duties described in this Procedure.

3.5 NOTIFICATION OBLIGATION UNDER OTHER LEGISLATION

This Procedure shall be enforced in addition to any applicable legal instrument and/or any applicable internal, contractual standard and procedure.

3.6 DOCUMENTATION AND RECORD KEEPING

As underlined by the Webhelp Information Security Policy:

All Security Incidents and suspected weaknesses shall be reported to the CISO via the locally documented procedures in order to allow Webhelp to: (…) (1) document Security Incidents and their outcomes (2) All information Security Incidents shall be investigated to establish their cause and impacts with a view to avoiding similar events.

In addition, to the above, the DPO shall document any Personal Data Breach in order to enable the Supervisory Authority to verify compliance with any Applicable Data Protection Legislation.

When Webhelp acts as a Data Controller or as a Data Processor, the following elements shall be adequately recorded within the documentation attached to any Data Protection Breach:

- The assessment conducted by the DPO
- The decision taken in response to a breach
- Attached to any relevant explanation in justification of a delayed notification
- Any exchange with Supervisory Authority and/or any communication to the Data Subject.
- Security Incidents and their outcomes

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

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

CATEGORIES OF PERSONAL DATA	DESCRIPTION
☐ **IDENTIFICATION DATA**	☐ Name, ☐ Surname, ☐ ID cards, Passport numbers ☐ Email ☐ Phone number ☐ Picture of a data subjet ☐ Postal address ☐ Video of the data subject ☐ Gender ☐ Other:
☐ **LIFE DATA**	☐ Life habit, Lifestyle ☐ Family status ☐ CV / Résumé ☐ Educational records ☐ Social care information ☐ Other:
☐ **ECONOMIC AND FINANCIAL DATA**	☐ Payment data ☐ Incomes / salary ☐ Financial situation ☐ Invoices ☐ Credit card data ☐ RIB/ IBAN ☐ Other:
☐ **TECHNICAL AND CONNEXION DATA**	☐ IP address ☐ Logs ☐ Device ID data ☐ Other:
☐ **DYNAMIC LOCALISATION DATA**	☐ Movement data ☐ Geo-localisation ☐ GPS data ☐ Other:
☐ **SENSITIVE DATA – SPECIAL CATEGORIES**	☐ Political opinion ☐ Biometric data ☐ Genetic data ☐ Racial or ethnic origin ☐ Religious or philosophical belief ☐ Trade union membership ☐ Sex life or sexual orientation ☐ Health related Data ☐ Criminal records ☐ ID numbers

Working Document 2

EXAMPLE	NOTIFY THE SUPERVISORY AUTHORITY	NOTIFY THE DATA SUBJECT ?	NOTES
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However if it is later compromised, notification is required.
Personal data of individuals are exfiltrated from a secure website managed by the controller during a cyber-attack. The controller has customers in a single Member State.	Yes, report to competent supervisory authority if there are potential consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high.	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed.
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable personal data breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the competent supervisory authority, if there are potential consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, the supervisory authority may consider an investigation to assess compliance with the

EXAMPLE	NOTIFY THE SUPERVISORY AUTHORITY	NOTIFY THE DATA SUBJECT ?	NOTES
			broader security requirements of Article 32.
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected..	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
A multi-national online marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.
A website hosting company (a data processor) identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive). If there is no evidence of this vulnerability being exploited with this particular controller a notifiable breach may not have occurred but is likely to be recordable or be a matter of non-compliance under Article 32.

EXAMPLE	NOTIFY THE SUPERVISORY AUTHORITY	NOTIFY THE DATA SUBJECT ?	NOTES
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Think Human

Webhelp SAS
161 Rue de Courcelles
75017 Paris
France

privacy@webhelp.com