1 SCOPE

Personal Data Incident Notification Policy

1.1 This personal data incident notification policy (the "Policy") applies to by The One-Shot Corporation, and its affiliates (together "**One-Shot**"). All Colleagues are required to follow this procedure in the event of a Personal Data Incident.

1.2 This Policy:

(a) forms part of One Shot's Data Protection Policy and

(b) may be amended by One Shot at any time, consistent with the requirements of applicable laws and regulations. Any revisions will take effect from the date on which the amended Policy is published, as indicated in the version number set out herein.

2 DEFINITIONS

2.1 "Colleague" is as defined in the Data Protection Policy;

"Data Subject" is as defined in the Data Protection Policy;

"**Data Protection Committee**" means the data protection committee of One-Shot which includes the Director responsible for Data Protection who may be contacted at privacy@one-shot.com and for GDPR purposes as set out in Schedule 1;

"IS" means the information systems department of One-Shot;

"Legal" means the Legal Representation of One Shot;

"Internal Breach Register" means the internal breach register which details any Personal Data Breaches;

"Personal Data" is as defined in the Data Protection Policy;

"pseudonymised data" means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person and "pseudonymised" and "pseudonymisation" shall be construed accordingly.

"Sensitive Personal Data" is as defined in the Data Protection Policy; and

"Supervisory Authority" means an independent public authority responsible for monitoring the application of the GDPR and other data protection laws.

2.2 Words denoting the singular shall include the plural and vice versa.

2.3 Unless otherwise stated, all defined terms have the same meaning as defined in the Data Protection Policy.

3 WHAT IS A PERSONAL DATA BREACH?

3.1 A "Personal Data Breach" is 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.

3.2 Examples of Personal Data Breaches are:

(a) "Confidentiality breach" – an unauthorised or accidental disclosure of or access to Personal Data;

(b) "Availability breach" – an unauthorised or accidental loss of access to or destruction of Personal Data;

(c) "Integrity breach" – an unauthorised or accidental alteration of Personal Data.

4 PERSONAL DATA BREACH AND PERSONAL DATA INCIDENT

4.1 Section 3.1 defines what a Personal Data Breach is.

4.2 A "Personal Data Incident" is a possible, potential or suspected Personal Data Breach. It is essential that you understand the distinction between a Personal Data Breach and a Personal Data Incident, i.e. a Personal Data Incident is not necessarily a Personal Data Breach.

4.3 If there has been a Personal Data Incident, any Colleagues involved should refer to the Personal Data Incident as an "incident" and should not refer to it as a "breach" (particularly when communicating in writing/by email).

4.4 It is for the Director in charge of Data Protection to determine whether a Personal Data Incident constitutes a Personal Data Breach.

5 PROCEDURE – ASSESSING A PERSONAL DATA INCIDENT

5.1 Notify Gary McGill

(a) One-Shot may be required to report Personal Data Breaches to the supervisory body no later than 72 hours after becoming aware of it. Due to this requirement, you must report all Personal Data Incidents (i.e. all possible, potential or suspected Personal Data Breaches) to Gary McGill immediately and in any event within 24 hours of becoming aware of the Personal Data Incident.

(b) If in doubt as to whether a Personal Data Incident or Personal Data Breach has occurred, you are required to err on the side of caution and report it.

(c) The Personal Data Incident notification needs to be made by phone and confirmed in writing by email:

(i) to the Director responsible for data protection (Gary McGill);

(ii) with a copy to the Data Protection Committee (at privacy@one-shot.com);

(iii) marked as "High Importance"; and

(iv) with the following in the Subject line: "Private, confidential and legally privileged – Personal Data Incident".

5.2 The Directors will confirm receipt of this information by email.

5.3 Each Personal Data Incident must have a risk assessment performed to determine the extent and risk to the Personal Data. The risk assessment is based on facts and determines whether the Personal Data was used or disclosed in a way not permitted under One Shot's policies. The risk assessment includes an evaluation of whether the incident compromises an individual's Personal Data.

5.4 For the risk assessment the following steps will be carried out:

(a) Data list:

A detailed list and description of the data involved in the Personal Data Incident needs to be prepared. The list must include all the Personal Data which is potentially at risk as a result of the incident.

(b) Security controls applied to the data:

Any security controls applied to the data may limit unauthorised exposure. This may include encryption, pseudonymisation, access controls or any other controls. The security controls applied to the data should be documented.

(c) Determination of risk to the individual:

The level of risk to the individual will determine whether the Personal Data Incident is to be notified to the Supervisory Authority and/or the affected Data Subject. Determining the risk requires an evaluation of:

(i) the facts surrounding the Personal Data Incident;

(ii) an examination of the type of Personal Data;

(iii) the potential harm to the individual; and

(iv) security controls applied.

(d) Forensic investigation:

IS is responsible for conducting computer forensics in support of investigations. IS must be engaged at the earliest opportunity when suspicious computer activity or security incidents occur to ensure information is properly gathered and handled during response efforts. No information (or structure of information) should be deleted, moved or changed in any way.

(e) Legal analysis:

The Directors will analyse the data identified under the 'data list', including the security controls applied and any risk to an individual, to consider whether the Personal Data Incident constitutes a Personal Data Breach.

5.5 The following factors (along with any other relevant considerations) will be considered to determine if Personal Data has been compromised (you need to ensure that this information is recorded and provided promptly in writing to the Directors):

(a) the nature of the Personal Data Incident including where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of data records concerned;

(b) the nature and extent of the Personal Data involved, including where Personal Data was pseudonymised data, types of identifiers and the likelihood of re- identification;

(c) the identity of the unauthorised person who triggered the Personal Data Incident and, where applicable, or to whom it was disclosed;

(d) whether the Personal Data was actually acquired (including whether any security controls were applied to prevent access);

(e) the likely consequences of the Personal Data Incident; and

(f) the measures that could be taken to address the Personal Data Incident, including

where appropriate, to mitigate any adverse effects.

5.6 If Personal Data is pseudonymised in accordance with applicable laws or guidance, it still qualifies as Personal Data and any inadvertent or unauthorised use or disclosure of such information will be considered a Personal Data Breach.

5.7 If Personal Data is anonymised in accordance with applicable laws and guidance, it is not Personal Data and any inadvertent or unauthorised use or disclosure of such information will not be considered a Personal Data Breach. Consult the Directors first to confirm if the data is truly anonymised.

5.8 It is important that systems and/or operations are restored as soon as possible, ensuring that this can be done without creating any further security issues or putting One Shot at risk of additional incidents or unintentionally discarding or destroying evidence.

5.9 Before any restoration of systems and/or data, the system should be tested to ensure it is no longer vulnerable or to prevent or minimise any potential future security risks.

6 PROCEDURE – BREACH NOTIFICATION TO SUPERVISORY AUTHORITY

6.1 If it is determined that the Personal Data Incident constitutes a Personal Data Breach, One-Shot will assess whether the Personal Data Breach is likely to result in a risk to the rights and freedoms of the Data Subjects affected by the Personal Data Breach, by conducting a Data Protection Impact Assessment. Such a risk if unaddressed is likely to have a significant detrimental effect on individuals – for example, resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

6.2 If a risk to Data Subject(s) is likely, One-Shot must report the Personal Data Breach to the Supervisory Authority without undue delay, and not later than 72 hours of becoming aware of the breach.

6.3 If it is not possible to provide all of the necessary information at the same time, One Shot will provide the information in phases without undue further delay. For the avoidance of doubt, even if all of the necessary information is not available, the Supervisory Authority must be contacted within the 72 hour deadline, and be provided with the information that is available and reasons why the remaining information is not available and expected timeframes when it will be provided.

6.4 The following information needs to be provided to the Supervisory Authority (you must ensure that this information is documented, so that it is available when required):

(a) a description of the nature of the Personal Data Breach;

(b) the date the Personal Data Breach occurred;

(c) the date the Personal Data Breach was discovered and any reasons why the breach was not notified within 72 hours (if applicable);

(d) the categories of Data Subjects affected;

(e) whether the Personal Data Breach involved pseudonymised data or anonymised data;

(f) approximate number of Data Subjects affected;

(g) the categories of Personal Data records affected;

(h) approximate number of Personal Data records affected;

(i) name and contact details of the Director responsible for Data Protection;

(j) the likely consequences of the breach; and

(k) any measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, to mitigate any adverse effects.

6.5 The Director responsible for Data Protection will notify the Supervisory Authority.

6.6 In the event the Supervisory Authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

6.7 The breach notification is made to the Supervisory Authority by email with a follow up telephone call.

7 PROCEDURE – BREACH NOTIFICATION TO DATA SUBJECT

7.1 If the Personal Data Breach is likely to result in high risk to the rights and freedoms of the Data Subject, One-Shot must notify the Data Subjects affected without undue delay.

7.2 The notification to the Data Subject should describe the breach in clear and plain language and contain at least the following information:

(a) name and contact details of the Director responsible for Data Protection;

(b) likely consequences of the Personal Data Breach; and

(c) measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, to mitigate any adverse effects.

7.3 Such notification to the Data Subject referred to is not required if:

(a) One-Shot has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption;

(b) One-Shot has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects referred are no longer likely to materialise; or

(c) it would involve disproportionate effort – in such a case, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

7.4 Consult the Director responsible for Data Protection first to confirm if any of the exceptions set out in Section 7.3 above apply.

8 INTERNAL REGISTER

One-Shot must keep an Internal Breach Register documenting any Personal Data Breaches which include:

(a) the facts relating to the Personal Data Breach;

(b) the effects of the Personal Data Breach; and

(c) the remedial action taken.

9 DOCUMENT CONTROL

9.1 Gary McGill is the owner of this Policy and is responsible for ensuring that this procedure is reviewed in line with the relevant review requirements.

9.3 This Policy was approved by the Directors in September 2018 and is issued on a version-controlled basis.