<

1. **Introduction**

This Policy sets out the Company name>>, a company registered in <<insert cou under number <<insert company registration number>>, w is at <<insert address>> ("the Company") regarding the h data breaches and personal data breaches in accordance on Legislation. "Data Protection Legislation", in this Policy, d regulations in force from time to time regulating the use of but not limited to, the retained EU law version of the Gener ulation ((EU) 2016/679) (the "UK GDPR"), as it forms part d Wales, Scotland, and Northern Ireland by virtue of section (Withdrawal) Act 2018, the Data Protection Act 2018, and a

The UK GDPR defines "pe rmation relating to an identified or identifiable natural person ntifiable natural person is one who can be identified, directly c by reference to an identifier such as a name, an identificatio , an online identifier, or to one or more factors specific to ical, genetic, mental, economic, cultural, or social identity o

The UK GDPR defines a "p a breach of security leading to the accidental or unlawful de , unauthorised disclosure of, or access to, personal data tra rwise processed.

The Company is under a d s of personal data breach directly to the Information Commis The Company is also required to inform individual data sub aches that present a high risk of adversely affecting their rig

All personal data collected y the Company will be handled in accordance with the Comp licy.

The Company has in place ection, investigation, and reporting of data breaches. This Po breaches (including personal data breaches) within the Comp assist in both the handling of such breaches and in determini ust be reported to the ICO and/or to data subjects.

[The Company's Data Pro name and contact details>>**] OR [**<<insert name and/or ontact details>>**] OR [**<<insert department>>, <<insert **OR [**are**]** responsible for the implementation of this Polic ndling of all data breaches, and for ensuring that this Policy is

2. **Scope of Policy**

2.1 This Policy relates t luding personal data and sensitive personal data (kn ory" under the Data Protection Legislation)) collect by the Company.

2.2 This Policy applies pany, including but not limited to employees, agents nts, temporary staff, casual or agency staff, or oth essors working for or on behalf of the Company.

2.3 This Policy applies ther suspected or confirmed.

3. Data Breaches

3.1 For the purposes each means any event or action (accidental or delib a threat to the security, integrity, confidentiality, or av

3.2 Incidents to which t clude, but not be limited to:

a) the loss or th cord;

b) the loss or ment (e.g. laptop), mobile devices (e.g. smartp e data storage devices (e.g. USB drive), or oth

c) equipment fa

d) unauthorised odification of data (or inadequate access contr d access, use, or modification);

e) unauthorised

f) human error wrong recipient);

g) unforeseen e or flood;

h) hacking, phis g" offences whereby information is obtained by

i) <<add furthe

4. Internal Reporting

4.1 If a data breach is d members of staff should complete a Data Breach Rep <<insert location>>) and send the completed form to Protection Officer**]** **OR [**<<insert name and/or positio tment>>**]**.

4.2 A completed Data B ld include full and accurate details about the incident in o (where applicable):

a) the time and

b) the time and covered;

c) the type(s) o

d) where the l data, the categories(s) of data subject to w elates (e.g. customers, employees etc.);

e) whether or n l data is involved;

f) how many d be affected (if known);

g) <<add furthe

4.3 Where appropriate, d liaise with <<insert position, e.g.

"their line manager" ata Breach Report Form.

4.4 If a data breach oc utside of normal working hours, it should be reported practicable.

4.5 Unless and until ins any's Data Protection Officer**] OR [**<<insert name and nsert department>>**]**, members of staff should not ta ith respect to a data breach. In particular, individua ld not take it upon themselves to notify affected da , or any other individuals or organisations.

5. **Initial Management and Reco**

5.1 Upon receipt of a D n (or upon being notified of a data breach in any oth y's Data Protection Officer**] OR [**<<insert name and sert department>>**]** shall begin by determining whethe till occurring. If this is the case, appropriate steps s ely to minimise the effects of the data breach and to

5.2 Having established g steps shall then be taken with respect to the data

a) undertake a the data breach, liaising with the relevant sta ere appropriate, to establish the severity of th

b) contain the e extent reasonably practicable, recover, am ailability of (e.g. by changing or revoking ac y temporarily making the data unavailable d data;

c) determine w can be done to recover the data and/or other amage caused by the breach;

d) establish wh tially (including, if physical records or equipmer n, the police) as part of the initial containment

e) determine, i nt staff and departments, the best course of ac dy the data breach; and

f) record the b os taken above in the Company's Data Breach

5.3 Having completed ed above, **[**the Company's Data Protection Officer**]** and/or position>>**] OR [**<<insert department>>**]** shal ng and assessing the data breach as described in Par

6. **Investigation and Assessme**

6.1 **[**The Company's r**] OR [**<<insert name and/or position>>**] OR [**<< ll begin an investigation of a data breach as soon a e after receiving a Data Breach Report Form (or be way) and, in any event, within 24 hours of the data br nd/or reported.

6.2 Investigations and a he following into account:

a) the type(s) n particular, whether the data is personal dat ata);

b) the sensitivit ercially and personally);

c) what the dat

d) what organi easures were in place to protect the data;

e) what might as a result of a breach (including unlawful or c isuse);

f) where perso at that personal data could tell a third party a whom the data relates;

g) the category ubject to whom any personal data relates;

h) the number roximate number if calculating an exact numbe ticable) likely to be affected by the data breach;

i) the potential cts involved;

j) the potential ompany;

k) the broader ata breach, both for data subjects and for the C

l) <<add furthe

6.3 The results of the sment described above must be recorded in the Com gister.

6.4 Having completed ssessment described above, **[**the Company's Data Pr nsert name and/or position>>**] OR [**<<insert departme he parties to be notified of the breach as describe

7. **Notification**

7.1 **[**The Company's r**] OR [**<<insert name and/or position>>**] OR [**<< ll determine whether to notify one or more of the follo :

a) affected data

b) the ICO;

c) the police;

d) the Compan

e) affected com

f) <<add furthe

7.2 When considering tify individual data subjects in the event of a personal g should be considered:

a) the likelihoo ts and freedoms as set out in the Data Prote the Company's Data Protection Policy) will b

b) whether ther l requirement to notify;

c) whether mea ct the affected personal data (e.g. pseudonymi e been applied, thereby rendering the data unu d parties;

d) whether mea following the data breach that will ensure that s and freedoms of affected data subjects is n

e) the benefits ing notified (e.g. giving them the opportunity t d by the data breach);

f) whether not nvolve disproportionate effort (in which case or other widely available notice may suffice, data subjects will still be informed effectively);

g) the best way ts, taking into account the urgency of the situati possible methods;

h) any special le to certain categories of data subject (e.g. eople);

i) the informati ed to affected data subjects;

j) how to make subjects to contact the Company to find out m h;

k) further assis y should provide to the affected data subject

l) the risks of data breaches require notification and excessi ult in disproportionate work and numbers of ;

m) <<add furthe ired>>.

7.3 When individual da nformed of a data breach, those individuals must be without undue delay. Individuals shall be provided wi on:

a) a user-friend a breach, including how and when it occurred, t d, and the likely consequences;

b) clear and sp vant, on the steps individuals can take to prote

c) a descriptio en (or proposed to be taken) to address the where relevant, measures taken to mitigate any ;

d) contact deta Data Protection Officer**] OR [**an individual o Company**]** from whom affected individuals c tion about the data breach.

7.4 When considering w tify the ICO of a data breach, the following should be

a) the risk and ubjects, their rights, and freedoms – harm can to) financial harm, physical harm, loss of contr scrimination, identity theft or fraud, damage to r distress;

b) the volume d – the ICO should be notified if a large volume there is a real risk of data subjects

suffering har t may also be appropriate to notify the ICO if a s sk data is involved;

c) the sensitivi - the more sensitive the personal data is, the s relevant and if the data breach presents a a subjects suffering substantial detriment or be notified.

7.5 If the ICO is to be n this must be done within 72 hours of becoming aware asible. This time limit applies even if complete details ot yet available. The ICO must be provided with the fo

a) the category pproximate number of data subject whose perso e data breach;

b) the category approximate number of personal data records

c) the name a **[**the Company's Data Protection Officer**] OR** rtment within the Company**]** from which the IC rmation about the data breach;

d) a description ces of the data breach; and

e) a descriptio en (or proposed to be taken) to address the where relevant, measures taken to mitigate any .

7.6 The police may ha n earlier point in the data breach procedure (see 5.2 tigation may reveal that the data breach resulted fro case the police should be further informed.

7.7 Records must be k regardless of whether notification is required. The de surrounding notification should be documented and re Data Breach Register.

8. Evaluation and Response

8.1 When the steps se completed, the data breach has been contained, a s notified, **[**the Company's Data Protection Officer**]** and/or position>>**] OR [**<<insert department>>**]** sha eview of the causes of the data breach, the effective ken in response, and whether any systems, policies, hanged to prevent data breaches from occurring in th

8.2 Such reviews shall the following with respect to data (and in particular, ed, held, and processed by the Company:

a) where and h ed;

b) the current ical security measures in place to protect data possible weaknesses of those measures;

c) the methods both physical and electronic data and whether secure;

d) the level of [illegible] lace and whether or not that level is necessary;

e) whether an[illegible] pact assessments need to be conducted o[illegible];

f) staff awaren[illegible] ing data protection;

g) <<add additi[illegible] sired>>.

8.3 Where possible in[illegible] her changes are identified, **[**the Company's Data Pr[illegible] nsert name and/or position>>**] OR [**<<insert departme[illegible] <<insert name and/or position>>**] OR [**<<insert depar[illegible] nt staff **[**and/or departments**]]** with respect to the imple[illegible] vements and/or changes.

9. **Policy Review and Implemen[illegible]**

9.1 This Policy will be[illegible] to reflect current best practice, official guidance, an[illegible] slation.

9.2 This Policy shall be[illegible] f <<insert date>>. No part of this Policy shall have [illegible] shall thus apply only to matters occurring on or afte[illegible]

This Policy has been approved an[illegible]

Name: <<insert[illegible]

Position: <<insert[illegible]

Date: <<insert[illegible]

Due for Review by: <<insert[illegible]

Signature: