Winder Research and Development Ltd

PERSONAL DATA BREACH POLICY

Last updated: 8 August 2022

1. DEFINITIONS

1.1 "**Data Protection Law**" means the UK GDPR, the Data Protection Act 2018 and any applicable national privacy legislation from time to time in force;

1.2 "**UK GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation); and

1.3 The terms "**data subject**", "**personal data**", "**processing**" and "**personal data breach**" have the meanings given to them in the UK GDPR.

2. INTRODUCTION

2.1 Winder Research and Development Ltd ("**Company**", "**our**", "**we**", "**us**") processes personal data according to Data Protection Law.

2.2 To comply with the principle of integrity and confidentiality under the UK GDPR, we have implemented technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3. ABOUT THIS POLICY

3.1 This policy ("**Policy**") sets out the Company's response plan for addressing personal data breaches under Articles 33 and 34 of the UK GDPR. It also explains our procedures for preventing personal data breaches and the process for ongoing improvements to reduce the risk.

3.2 This Policy applies to all categories of personal data processed by the Company, whether relating to staff, contractors, customers, clients or any other third party.

3.3 This Policy applies to all staff unless otherwise stated but does not form part of the terms of any contract a staff member has with the Company, which are provided separately. In the event of any conflict between this Policy and the terms of a staff member's contract, the latter will prevail.

3.4 Staff members are required to familiarise themselves with the contents of this Policy and comply with it at all times. Breach of this Policy or of any Data Protection Law may result in disciplinary action up to and including dismissal.

3.5 The Phil Winder has overall responsibility for this Policy and ensuring that it meets the Company's legal obligations. Any questions about the contents of this Policy should be directed to Phil Winder.

4. PERSONAL DATA BREACHES

4.1 For the purposes of this Policy, personal data breaches include both confirmed and suspected incidents which have compromised, or have the potential to compromise, the confidentiality or availability of systems or data.

4.2 Examples of personal data breaches may include:

4.2.1 loss or theft of data or equipment on which data is stored (eg laptop, USB stick or paper files);

4.2.2 unauthorised use of, access to, or modification of confidential data;

4.2.3 loss of availability of personal data;

4.2.4 unauthorised disclosure of sensitive or confidential personal data;

4.2.5 equipment or system failure;

4.2.6 ‘phishing’ scams where information is obtained by deceiving the Company;

4.2.7 hacking attack;

4.2.8 human error; or

4.2.9 unforeseen circumstances such as a fire or flood.

5. PREVENTING A PERSONAL DATA BREACH

5.1 We are committed to processing personal data securely and have put in place preventative measures to reduce the risk of a personal data breach.

5.2 The Company will provide mandatory data protection training to all staff on induction and as required thereafter. This training will cover personal data breaches, including how to recognise a breach when it occurs and the importance of following the Company’s reporting procedure.

5.3 Staff with responsibility for personal data or whose work involves dealing with personal data on a regular basis will be required to complete additional training. Managers must ensure that they and their staff have completed any required data protection training courses.

6. PROCEDURE FOR REPORTING A PERSONAL DATA BREACH

6.1 Any individual who accesses or uses the Company’s IT systems is responsible for reporting actual, threatened, suspected or potential personal data breaches and security incidents immediately (a “**Breach Report**”). If the incident occurs or is discovered outside normal working hours, it must be reported as soon as possible.

6.2 Staff should report actual or potential personal data breaches to the CEO at phil@winder.ai.

6.3 Breach Reports should contain full and accurate details of the incident, the date and time it occurred, the nature and volume of the personal data affected, how many individual data subjects are involved and the identity of the person who triggered the breach.

7. RESPONSE PLAN

7.1 Initial assessment

7.1.1 On receipt of a Breach Report, the CEO will make an initial assessment to establish the severity of the breach and determine whether any personal data is involved.

7.1.2 The CEO will then decide who will be the Lead Investigating Officer ("**LIO**") in charge of managing the breach.

7.2 Containment

7.2.1 The LIO will identify the cause of the breach and whether it has been contained.

7.2.2 If the breach is still occurring, the LIO will take appropriate steps to minimise the effect of the breach and consider whether anything can be done to recover any losses.

7.2.3 The LIO will establish who may need to be notified of the personal data breach.

7.3 Investigation and risk assessment

7.3.1 The LIO will investigate the breach immediately and, where possible, within 24 hours of receiving the Breach Report.

7.3.2 The risk assessment will include consideration of:

(a) the type of data involved and its sensitivity;

(b) what has happened to the data;

(c) whether there were existing security controls in place;

(d) the number of individuals affected;

(e) whether the data could be used illegally;

(f) whether there could be any harm to individuals; and

(g) the wider consequences such as damage to reputation.

7.3.3 The LIO will produce a report summarising the findings of the investigation and risk assessment.

7.4 Notification to supervisory authority

7.4.1 The LIO and/or the CEO will consider whether the Company must notify the Information Commissioner's Office ("**ICO**"), by establishing the likelihood and severity of the risk to the rights and freedoms of those affected by the breach.

(a) If it is likely that there will be a risk to the rights and freedoms of individuals, the Company shall notify the ICO within 72 hours of the Company becoming aware of the breach as set out in clause 7.4.2.

(b) If it is unlikely that there will be a risk to the rights and freedoms of individuals, the Company will not notify the ICO. In this case the LIO must document the reasons for the decision not to notify, including all the relevant factors and information about the breach, and keep a record of this.

7.4.2 Notifications to the ICO will include:

(a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects and personal data records concerned;

(b) the name and contact details of the Phil Winder;

(c) a description of the likely consequences of the personal data breach; and

(d) a description of the measures taken, or proposed, to deal with the breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

7.5 Notification to individuals

7.5.1 The LIO and/or the CEO will consider whether the Company must notify the individuals affected by the breach.

7.5.2 Subject to clause 7.5.4, where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will inform the affected individuals without delay.

7.5.3 Notifications to individuals will explain, in clear and plain language, the nature of the personal data breach. They will also contain at least the information in clause 7.4.2(b), 7.4.2(c) and 7.4.2(d).

7.5.4 Individuals will not be notified where:

(a) appropriate technical and organisational measures have already been applied to the personal data affected by the breach (eg encryption);

(b) measures have already been taken which ensure that the high risk to the rights and freedoms of individuals is unlikely to materialise; or

(c) to do so would involve disproportionate effort, in which case there shall be a public communication or similar measure instead.

7.6 Evaluation and response

7.6.1 Once the particular personal data breach has been contained, the LIO and/or the CEO shall carry out a full review of the cause of the breach and the effectiveness of the response.

7.6.2 The review will consider the adequacy of existing controls, any corrective action required, how personal data is held, where the biggest risks lie and whether staff are sufficiently aware of how to recognise and respond to a personal data breach.

7.7 Record-keeping

7.7.1 The LIO and/or the CEO shall document and keep records of all personal data breaches and incidents, regardless of whether or not the breach was reported to the ICO.

7.7.2 Such records shall include the facts relating to the breach, the effects of the breach and the action taken to remedy the breach.