Version 1.0

Data Breach Notification Policy

At PHD INTERACTIVE LTD T/A WEBHEALER, we take the security and privacy of personal data seriously. Despite our strong security measures, we recognize that data breaches can occur. In compliance with the UK GDPR, we have established a data breach response plan to handle such incidents swiftly and responsibly.

1. Identification of a Data Breach

A **data breach** occurs when personal data is lost, stolen, accessed without authorization, or otherwise compromised. This includes incidents such as hacking, unauthorised access, accidental loss, destruction, or alteration of personal data.

Upon discovering a potential or confirmed data breach, we will immediately take the following steps:

- **Containment and Mitigation**: We will quickly assess the situation, contain the breach, and take measures to prevent further data loss. This may include disabling compromised systems, revoking access rights, or isolating affected data.

- **Assessment**: We will assess the scope and severity of the breach to determine whether personal data has been compromised, the type and volume of data affected, and the potential risks to individuals' rights and freedoms.

2. Notification to the Supervisory Authority

If we determine that a personal data breach has occurred that poses a risk to individuals' rights and freedoms, we will notify the relevant supervisory authority, the **Information Commissioner's Office (ICO)**, within **72 hours** of becoming aware of the breach. This notification will include:

- A description of the nature of the breach, including the categories and approximate number of data subjects and personal data records affected.
- The name and contact details of our Data Protection Officer (or relevant point of contact).
- A description of the likely consequences of the breach.
- A description of the measures we have taken or propose to take to address the breach and mitigate its potential adverse effects.

If we are unable to provide all the necessary information within 72 hours, we will provide an initial notification and follow up with additional details as they become available.

3. Notification to Affected Individuals

If the breach is determined to be **high risk**—meaning it is likely to result in significant harm or impact to individuals' rights and freedoms—we will notify the affected individuals **without undue delay**. This notification will include:

- A clear description of the nature of the breach.
- The contact information of our Data Protection Officer or other relevant points of contact.
- A description of the potential consequences for the affected individuals.
- The specific steps that affected individuals can take to protect themselves (such as changing passwords or monitoring for fraudulent activity).
- The measures we have taken or will take to mitigate the impact of the breach.

If it is not possible to notify each affected individual directly, we will take other measures, such as issuing a public communication or posting a notice on our website.

4. Notification to Clients (Data Controllers)

As a **Data Processor**, if we experience a breach involving personal data that we process on behalf of our clients (Data Controllers), we will notify the affected clients **without undue delay**. This notification will include:

- A detailed description of the nature of the breach.
- The categories of data affected and the potential risk to individuals' privacy.
- The corrective actions we are taking to contain and mitigate the breach.
- Guidance on how clients can inform and assist their own customers (data subjects) if required.

5. Post-Breach Actions and Review

Following a data breach, we will:

- **Mitigate Further Damage**: We will implement additional measures to ensure that the breach is contained and prevented from spreading. This may include patching security vulnerabilities, strengthening access controls, or isolating compromised systems.
- **Investigation and Root Cause Analysis**: We will conduct a thorough investigation into the cause of the breach, identify any weaknesses in our security protocols, and implement appropriate corrective actions.

- **Review and Improve Security Practices**: Following the breach, we will assess and update our security policies, practices, and procedures as necessary to prevent similar incidents in the future. We will also provide additional training to staff as needed.

6. Record Keeping

In compliance with GDPR, we will document all breaches, regardless of whether they require notification to the ICO or individuals. This record will include:

- The facts surrounding the breach.
- Its effects.
- The remedial actions taken.

This documentation helps demonstrate our compliance with GDPR requirements and provides insights into how we can improve our data protection processes.