Paddle UK Data Breach Policy

1. POLICY STATEMENT

1.1. Paddle UK[1] holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. The policy applies to all personal and sensitive data held by Paddle UK and all staff, board members, volunteers and contractors, referred to herein after as 'workers'.

2. PURPOSE

2.1. This policy outlines the course of action to be followed by all workers at Paddle UK if a data protection breach takes place.

3. WHAT IS A DATA BREACH

3.1. The retained EU law version of the General Data Protection Regulation (UK GDPR) defines a 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”. A data breach can be accidental or deliberate and can be broadly deemed to be an incident which has impacted upon the confidentiality, integrity or availability of personal data.

4. LEGAL CONTEXT

4.1. Article 33 of the UK GDPR outlines the legal position regarding data breaches and in particular the notification of a personal data breach to the supervisory authority.

4.2. Article 33 outlines:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO) which is the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

    a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and

[1] Paddle UK is a trading name of British Canoeing which is a Company registered at Companies House with the registered number 01525484.

the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

f) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

5. TYPES OF BREACH

5.1. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

5.1.1. Loss or theft of staff, or Paddle UK data and/ or equipment on which data is stored;
5.1.2. Inappropriate access controls allowing unauthorised use;
5.1.3. Equipment Failure;
5.1.4. Loss of availability of data;
5.1.5. Poor data destruction procedures;
5.1.6. Human Error including sending personal data to an incorrect recipient or alteration of personal data without permission;
5.1.7. Cyber-attack;
5.1.8. Hacking.

6. MANAGING A DATA BREACH

6.1. In the event that Paddle UK identifies or is notified of a personal data breach, the following steps should followed:

6.1.1. The person who discovers/receives a report of a breach must inform the Data Protection Officer (DPO) or their nominated representative without undue delay. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

6.1.2. The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert

relevant staff such as the IT Support Service Manager or Director of Digital Transformation and IT.

6.1.3. The DPO (or nominated representative) must inform the Chief Executive as soon as possible. As a registered Data Controller, it is the Paddle UK's responsibility to take the appropriate action and conduct any investigation.

6.1.4. The DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, external legal advice may be required.

6.1.5. The DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Such steps might include:

6.1.5.1. Attempting to recover, or remotely wipe, lost or stolen equipment.

6.1.5.2. Contacting all relevant Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information.

6.1.5.3. Depending on the severity of the breach, consideration should be given to a global email to all staff or where the breach is sufficiently serious, the wider workforce. If an inappropriate or unexpected enquiry is received by a member of staff, or any worker, they should attempt to obtain the enquirer's name and contact details and not share any further personal or confidential information until their identity is properly verified. Whatever the outcome of the call, it should be reported immediately to the DPO (or nominated representative).

6.1.5.4. Contacting Paddle UK's Communications team if the breach is severe, as they may need to be prepared to handle any press enquiries. The Paddle UK's Director of Business Development and Communications, Rob Knott can be contacted on Tel: 0115 8966582 or via email at robert.knott@paddleuk.org.uk

6.1.5.5. The use of back-ups to restore lost/damaged/stolen data.

6.1.5.6. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

6.1.5.7. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and workers informed.

7. INVESTIGATION

7.1. In most cases, the next stage would be for the DPO (or nominated representative) to fully investigate the breach. The DPO (or nominated representative) should

ascertain whose data was involved in the breach, the potential effect on the data subject(s) and what further steps need to be taken to remedy the situation. The investigation should consider:

7.1.1. The type of data;
7.1.2. Its sensitivity;
7.1.3. What protections were in place (e.g., encryption);
7.1.4. What has happened to the data;
7.1.5. Whether the data could be put to any illegal or inappropriate use;
7.1.6. How many people are affected;
7.1.7. What type of people have been affected (members, workers, suppliers etc) and whether there are wider consequences to the breach.

7.2. A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been initially resolved.

8. NOTIFICATION

8.1. Some people/agencies may need to be notified as part of the initial containment operation. However, any decision in this regard will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

8.2. When notifying individuals, clear and specific advice should be given on what they can do to protect themselves and what Paddle UK is able to do to help them. They should be given the opportunity to make a formal complaint if they wish. The notification should include a description of how and when the breach occurred and what data was involved as well as including details of what has already been done to mitigate the risks posed by the breach.

9. REVIEW AND EVALUATION

9.1. Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team and Board meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach involves a staff member and warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach policy may need to be reviewed after a breach, legislative changes, new case law or new guidance.

10. IMPLEMENTATION

10.1. The DPO should ensure that workers are aware of the Paddle UK's Data Protection Policy and this Paddle UK Data Breach Policy. This should be undertaken as part of induction, supervision and ongoing training. If workers have any queries in relation to these, or any associated polices or procedures, they should discuss this with their line manager or the DPO.

11. CONTACT

11.1. The DPO is responsible for ensuring compliance with the Data Protection Laws and with this policy. Within Paddle UK, this post is held by Nancy Squires, Director of Governance (nancy.squires@paddleuk.org.uk). Any questions about the operation of this policy or any concerns or reports should be referred in the first instance to the DPO or via gdpr@paddleuk.org.uk.