PROFILE PILOT

PERSONAL DATA BREACH INCIDENT RESPONSE PROCEDURE

Background

A personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Profile Pilot is committed to the obligations in accordance with the GDPR. We are progressing towards our goal to maintain a robust and structured program for compliance adherence and monitoring to ensure that the correct procedures, controls and measures are in place where necessary. However, breaches can still occur, so this procedure states our intent and objectives for dealing with such data breaches involving personal information.

Objectives

- To adhere to the GDPR and other Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Personal Data Breach Incident Form for all personal data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect all on board on Profile Pilot platform – including their data, information and identity
- To ensure that the Supervisory Authority is notified of the data breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach

Key Concepts

Personal Information

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source and regardless of whether it is publicly available.

Data Breach

A personal data breach occurs when personal information is subjected to unauthorized access or disclosure, or where the information is lost and unauthorized access or disclosure is likely to occur.

Data breaches resulting from human error:

- Loss of employee's laptop, USB or paper records that contain personal information (e.g. left on a train, at the airport, stolen from the car etc.)
- Employee accidentally disclosing personal information to the wrong recipient or exposing any resource containing personal information to wrong recipients or to the public, sending correspondence with personal or sensitive information to the wrong person etc.

Data breaches resulting from malicious activity:

- Hacking into employee's email accounts, software, applications or datasets etc containing Personal Information
- Scams that trick employees into releasing personal information
- Inappropriate or fraudulent use of datasets containing personal information

Data breaches resulting from unforeseen circumstances:

- Unforeseen events that occur to Profile Pilot or to any Third party who holds personal information on behalf of Profile Pilot or if a cloud service provider suffers a data breach

Eligible Data Breach

An eligible data breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates, in which case Profile Pilot must inform either the data controller or the Supervisory Authority and affected data subject(s) depending on Profile Pilot's role.

Key Roles and Responsibilities

Profile Pilot Employee

- Report incidents immediately to their Manager
- Complete the Data Breach Report and give to Manager
- Participate in investigations as required

Manager (head of the relevant function)

- Receive Data Breach Reports from Profile Pilot employees within their area
- Contain breach, remediate harm, and preserve evidence
- Forward Data Breach Report to the Data Privacy/Protection Officer
- Assist with investigations as required

Data Privacy/Protection Officer

- Receive Data Breach Reports from Manager and alerts CTO of potential data breach
- Conduct a preliminary investigation
- Provide findings to CTO and alerts legal personnel
- Participate as a member of the Data Breach Response Group

- Record incidents and proceedings in the Non-Compliance Register

Chief Technology Officer (CTO)

- Receive preliminary investigation findings from Data Privacy/Protection Officer
- Determine the seriousness of the data breach
- Decide whether to convene the Data Breach Response Team and whether to include additional members
- Approve assessment by Data Breach Response Team
- Make notifications as appropriate
- Conduct post-action review

Data Breach Response Team

- Assess preliminary investigation
- Assess containment and/or remediation actions
- Assess whether an eligible data breach has occurred
- Assess notification requirements
- Assist with post-action review

Timeframes

An actual or suspected data breach must be investigated and managed as soon as any Profile Pilot employee becomes aware of the data breach, or suspects that it has occurred.

Assessment must be reasonable and expeditious. All reasonable steps to complete the assessment within 30 days of the date that Profile Pilot became aware of an eligible or suspected data breach. This timeframe should be treated as the maximum timeframe for completing the assessment.

Profile Pilot as Data Controller: Notify the Supervisory Authority and affected data subject(s) as soon as practicable after becoming aware of an eligible data breach. The Supervisory Authority is notified of the breach no later than 72 hours and is kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes. If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay.

Profile Pilot as Data Processor: The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

– Report and Contain

Personal Data Breach Reporting

If any Profile Pilot employee becomes aware of an actual or suspected data breach, they must report it as soon as possible. Reporting incidents in full and with immediate effect is essential so that breach procedures can be initiated and followed without delay. These procedures are for the protection of Profile Pilot, its employees, partners, vendors, customers and third parties and are very important for legal regulatory compliance. They should immediately:

1. Record the details of data breach
2. Provide a copy of this Data Breach Report to direct Manager
3. Keep it confidential except where it is necessary to disclose information about the incident

Containing Data Breaches and Remediating Harm

As soon as a breach is reported, the Manager is responsible for taking immediate action to contain the breach and remediate harm, including by seeking assistance from the appropriate business functions or third parties as necessary. At any time, appropriate steps should be taken to reduce any potential harm to affected data subjects.

Remedial actions are not in the scope of this document due to the vast nature of breaches and the variety of actions that can be taken; however, the aim of any such actions should be to stop any further risk/breach. The actions taken are noted on the incident record in all cases.

Preserving Evidence of a Suspected Data Breach

The Manager must take any reasonable steps available to them to preserve and/or record evidence of an actual or suspected data breach and provide this Data Breach Report with remedial action details to the Privacy/Protection Officer.

– Investigate

Preliminary Investigation

The Data Privacy/Protection Officer must review this report of an actual or suspected data breach as soon as reasonably practicable. Data Privacy/Protection Officer must:

1. notify the CTO that a data breach report has been received
2. assess what containment and/or remediation actions have already been taken by manager (if any) and whether any further actions are required
3. undertake any preliminary investigations necessary to confirm the report and/or seek any clarification or additional details

Initial Assessment

Once the report has been reviewed and preliminary investigation is done to confirm the incident, the Data Privacy/Protection Officer must make an initial assessment of:

1. whether the reported incident is a data breach or not (such that a further investigation is required or not)

---

2. If there is a data breach, give an initial risk rating to all relevant areas of impact including:
    a. number of data subjects affected by the breach or suspected breach;
    b. type of personal information;
    c. likelihood of serious harm to affected data subjects;
    d. Incident indicates a problem in Profile Pilot's processes, systems, products or services;
    e. Whether remedial actions have successfully prevented harm to affected data subjects

Reporting

The Data Privacy/Protection Officer must provide the findings of the preliminary investigation to the CTO as soon as possible.

– Assessment

Escalation to Data Breach Response Team

The CTO will assess the preliminary investigation findings to determine whether to convene the Data Breach Response Team. The CTO may request further information if required, to make this determination. If the CTO:

1. determines the incident is not a data breach, it will not be escalated to the Data Breach Response Team and The CTO will direct Manager and Data Privacy/Protection Officer to take any action reasonably necessary to close-out the incident appropriately;
2. determines the incident is a data breach and serious harm is possible, it should be escalated to the Data Breach Response Team for further assessment;
3. determines the incident is a data breach and serious harm is at most unlikely, it should not be escalated to the Data Breach Response Team. The CTO will direct the Manager and Data Privacy/Protection Officer to take any action reasonably necessary to close-out the incident appropriately and record the incident in the Risk Register.

Data Breach Response Team

The Data Breach Response Team comprises the following permanent members: CTO (or nominee), Data Privacy/Compliance (or nominee), Risk (or nominee), IT Security and Architecture (or nominee). CTO may co-opt additional members onto the Data Breach Response Team or engage external providers to assist in containment or investigation of the breach, depending on the nature or severity of the data breach.

Data Breach Assessment

If the incident is escalated to the Data Breach Response team then the Data Breach Response Team must have a secure meeting as soon as possible to discuss the Data Breach Report and the results of the preliminary investigation (including any containment and/or remediation steps taken). The Data Breach Response Team is responsible for assessing and determining whether:

1. the data breach is likely to result in serious harm to the affected data subject(s)

2. mandatory notification to Supervisory Authority and affected data subject(s) is required or
3. if notification is not mandatory, voluntary notification to Supervisory Authority and affected data subject(s) is desirable

Record Keeping and Evidence Preservation

Data Breach Response team must keep records of all steps taken in response to the data breach and decisions made in connection with it. This includes:

1. keeping a record of all steps taken during the preliminary investigation and subsequent assessment of the reported data breach; and
2. ensuring that any relevant evidence of the data breach (such as snapshots, forensic or other investigative processes) is preserved and stored securely.

The information may be required by the investigators, legal advisors, law enforcement and regulators, as well as for use in preparing notifications to and communications with affected individuals and the Supervisory Authority and any other regulator or relevant entities. Evidence and records must be sufficient to demonstrate to the Supervisory Authority the reasonable steps taken to comply with statutory and other legal obligations.

– Notification

Non-eligible Data Breaches

If the CTO determines the data breach is not an eligible data breach, the Data Privacy/Protection Officer will record the incident in the risk register and undertake action that is reasonably necessary to close-out the incident appropriately along with the Area Manager.

Eligible Data Breaches

Profile Pilot as Data Processor: If an eligible breach has occurred exposing personal information which was collected by a data controller and then Profile Pilot being in the role of data processor only, should notify the controller without undue delay after becoming aware of a personal data breach. It is the data controller's responsibility to notify the Supervisory Authority and affected data subject(s) (Article 33 GDPR). Also, It is equally important to review the Data Protection Agreement between controller and processor (Profile Pilot) to check for any contractual obligations agreed in the event of a personal data breach and its notifications (Article 28 GDPR).

Profile Pilot as Data Controller: If an eligible breach has occurred exposing personal information which was collected and processed by Profile Pilot, then It is mandatory for Profile Pilot to notify the Supervisory Authority (Information Commissioner) and affected data subject(s) as soon as practicable after becoming aware of an eligible data breach. The Supervisory Authority is notified of the breach no later than 72 hours and is kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

Notification to Supervisory Authority

Online notification submission is preferred by most of the regulatory authorities worldwide. It is mandatory to include the following information in the notification:

1. the identity and contact details of the data controller (Profile Pilot);
2. a description of the eligible data breach;
3. kind(s) of Personal Information affected by the breach;
4. categories of the data subjects affected; and
5. recommended steps that data subject(s) should take to protect their position in response to the data breach.

It is optional to include the following additional information in the initial report like:

1. details about the circumstances of the breach;
2. number of data subject(s) affected;
3. additional information about the steps taken to respond to the breach; and
4. any other information that might be relevant to assist Supervisory Authority in considering the appropriate response to the notification.

Notification to affected Data Subject(s)

The Data Breach Response Team is responsible for preparing a draft notification and assessing the options available for notifying affected data subject(s) of the data breach. The notification to affected data subject(s) must include:

1. how and when a data breach happened;
2. the types of the Personal Information involved in the data breach;
3. what steps have been taken and what will be taken to reduce or eliminate the risk of harm brought about by the data breach;
4. any assurances (if applicable) about what data has not been disclosed;
5. what steps the data subject(s) can take to protect themselves and what Profile Pilot will do to assist them (if applicable);
6. contact details of Profile Pilot for questions or requests for information or assistance;
7. whether Supervisory Authority has been notified about the data breach; and
8. how a data subject can lodge a privacy complaint with the Supervisory Authority.

Additional Notifications

There may also be other notifications which would be appropriate in the particular circumstances (e.g. notifying insurers, the police, cybercrime agencies etc.). If the Data Breach Response Team determines that additional notification is desirable, approval must be obtained from the CTO before such notification is made.

– Review

Post Breach Review

The CTO is responsible for conducting a post-breach review and assessment, once the immediate consequences of the data breach have been dealt with. In conducting the review, the CTO:

1. should seek informal input and assistance from other members of the Data Breach Response Team and other business units, as required;
2. must:
    a. complete any further investigations as necessary or desirable;
    b. determine whether any data handling or data security practices led or contributed to the relevant data breach;
    c. consider whether there are any further actions that need to be taken as a result of the relevant data breach, such as: updating security measures; reviewing and updating this data breach response plan; making appropriate changes to practices, systems, services, other processes, policies and procedures; revising training practices; reviewing partner, vendor or third party's security/contract terms and ongoing engagement; and considering undertaking an audit to ensure necessary outcomes are implemented.

Update Risk Register/Non-Compliance Register as appropriate, provide a written report for audit, compliance and risk with findings and recommendations for the further actions.