# ONMO Sweden AB
# Breach Notification Policy

Document Release Date: 2024
Document Version: 1.0
Document classification: External / Important

Document Control:

| | |
|---|---|
| Document Status | Draft |
| Document Classification | External / Important |
| Document Owner | Director – Information Technology |
| Effective Date | 26.12.2024 |
| Version | 1.0 |

Approval and authorization:

| **Name** | **Designation & Department** | **Date** |
|---|---|---|
| Ramani Gogoi | MR, Senior Manager – Information Technology | 26.12.2024 |
| Rajinder Sharma | General Counsel | 26.12.2024 |

onmobile

## 1. Introduction

This Breach Notification Policy (the "Policy") outlines the procedures and guidelines to be followed by **ONMO Sweden AB** (referred to as "we," "our," or "us") for handling and notifying individuals and regulatory authorities of any personal data breaches in compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

## 2. Definitions

2.1. Personal Data: Refers to any information relating to an identified or identifiable natural person (the "Data Subject") that we collect, process, store, or transmit.

2.2. Data Breach: Refers to a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

## 3. Reporting Breaches

3.1. Internal Reporting

3.1.1. Any employee, contractor, or authorized personnel who becomes aware of a potential data breach must immediately report it to the designated Data Protection Officer (DPO) or the incident response team.

3.1.2. Breach report should include as much information as possible, such as the date and time of the breach, the type of breach, the affected data subjects, and any other relevant details.

3.2. External Reporting

3.2.1. We assess the severity and risks associated with a data breach on a case-by-case basis, taking into account the nature, scope, context, and potential impact on individuals (GDPR Article 33(1)).

3.2.2. Where a breach results in a high risk to the rights and freedoms of individuals, we notify the Swedish Data Protection Authority ("IMY") without undue delay and within 72 hours after becoming aware of the breach (GDPR Article 33(1)).

3.2.3. We will cooperate and provide the IMY with all necessary information and documentation related to the breach as requested (GDPR Article 33(3)).

3.2.4. If the breach is likely to result in a high risk to the rights and freedoms of affected individuals, we will promptly notify those individuals, providing clear and concise information about the breach, the potential risks, and any recommended actions they should take (GDPR Article 34(1)).

## 4. Responsibilities

4.1. Data Protection Officer (DPO): Responsible for overseeing the response to data breaches and ensuring compliance with GDPR.

4.2. Incident Response Team: A group comprising IT, Legal, Compliance, and Communications departments, responsible for handling the breach response.

4.3. The responsibilities of Incident Response Team include:

4.3.1. Validate/triage the personal data breach

4.3.2. Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded

4.3.3. Identify remediation requirements and track resolution

4.3.4. Report findings to the top management

4.3.5. Coordinate with appropriate authorities as needed

4.3.6. Coordinate internal and external communications

4.3.7. Ensure that impacted data subjects are properly notified, if necessary

4.4. The Data Breach Response Team will convene for each reported (and alleged) personal data breach, and will be headed by the Data Breach Response Team Leader.

## 5. Breach Assessment and Investigation

5.1. Our incident response team, in collaboration with the DPO, will conduct a prompt and thorough assessment of the data breach to understand its nature, scope, and potential impact (GDPR Article 33(5)).

5.2. The investigation will include, but not be limited to:

5.2.1. Identifying the cause and extent of the breach.

5.2.2. Determining the categories and amount of personal data affected.

5.2.3. Assessing the potential consequences and risks to individuals.

5.2.4. Evaluating any potential mitigation measures or recovery steps to prevent further harm.

## 6. Notification Procedure:

6.1. Supervisory Authority Notification:

Notify the relevant supervisory authority within 72 hours of becoming aware of the breach, if the breach is likely to result in a risk to the rights and freedoms of individuals.

6.2. The notification should include:

6.2.1. Description of the nature of the breach

6.2.2. Categories and approximate number of data subjects and records affected

6.2.3. Contact details of the DPO

6.2.4. Likely consequences of the breach

6.2.5. Measures taken or proposed to address the breach

6.3. Data Subject Notification:

If the breach is likely to result in a high risk to the rights and freedoms of individuals, notify the affected data subjects without undue delay.

6.4. The notification should include:

6.4.1. Description of the nature of the breach

6.4.2. Name and contact details of the DPO

6.4.3. Likely consequences of the breach

6.4.4. Measures taken or proposed to address the breach

6.4.5. Notification methods can include direct communication (e.g., email, letter) and public announcements if individual notification is impractical.

## 7. Remediation and Mitigation

7.1. Upon identifying a data breach, we will take immediate action to mitigate any ongoing risks, minimize the impact, and prevent further unauthorized access or disclosure.

7.2. Remediation steps may include:

7.2.1. Implementing necessary technical and organizational measures to secure personal data.

7.2.2. Cooperating with law enforcement agencies, regulatory authorities, or third-party service providers, as required.

7.2.3. Conducting internal reviews and implementing measures to prevent similar breaches in the future.

## 8. Documentation and Record Keeping

8.1. We will maintain comprehensive records of all data breaches, including their nature, effects, and the remedial actions taken.

8.2. These records will include:

8.2.1. The date, time, and nature of the breach.

8.2.2. The scope and categories of personal data affected.

8.2.3. The individuals and supervisory authorities notified.

8.2.4. Any additional actions taken to mitigate risks and prevent future breaches.

## 9. Review and Updates

9.1. This Policy will be periodically reviewed and updated to ensure its effectiveness, compliance with GDPR, and any relevant changes in the regulatory framework.