Incident Response Plan — Momtivation App (LeadClosers d.o.o.)

Last updated: [insert date]

1. Introduction

This Incident Response Plan outlines the procedures LeadClosers d.o.o. will follow in the event of a personal data breach involving the Momtivation App, in accordance with GDPR Articles 33 and 34.

2. Definition of a Data Breach

A data breach includes:

- Unauthorized access to personal data
- Accidental or unlawful destruction, loss, alteration, or disclosure
- Unauthorized access to health or Apple Health data
- System compromise affecting confidentiality, availability, or integrity

3. Objectives of Incident Response

- Protect affected users
- Limit damage and prevent further data loss
- Restore normal operations quickly
- Ensure transparency with users and supervisory authorities
- Maintain full GDPR compliance

4. Incident Response Phases

1) Detection

2) Assessment

3) Containment

4) Notification

5) Recovery

6) Post-incident review

5. Detection of Incidents

Incidents may be detected through:

- System monitoring and logs

- Security tools and anomaly detection

- Reports from users

- Reports from subcontractors or partners

All incidents must be immediately escalated to the responsible personnel.

6. Initial Assessment

The assessment must determine:

- Whether personal data was affected

- Whether sensitive data (health data, Apple Health) was involved

- Approximate number of users impacted

- Whether risks to rights and freedoms are likely

Risk levels:

- Low

- Medium

- High (triggers user notification)

7. Containment Measures

Depending on severity:

- Disable compromised accounts

- Block unauthorized access

- Reset passwords

- Suspend affected systems

- Patch vulnerabilities

8. Notification Obligations

8.1 Notification to Supervisory Authority (AZOP)

If the breach is likely to pose a risk to users, AZOP must be notified within **72 hours**.

Notification must include:

- Description of the breach

- Categories and number of affected users

- Consequences of the breach

- Measures taken to mitigate impact

8.2 Notification to Users

If high risk exists, users must be notified without delay.

Notification must include:

- Clear description of the incident

- Possible consequences

- Recommended user actions

- Contact details

9. Recovery

Actions include:

- Restoring secure system functionality
- Verifying integrity of restored data
- Enhancing security configurations
- Monitoring for recurrence

10. Documentation of Incidents

Each breach must be documented with:

- Date/time discovered
- Nature of the breach
- Categories of affected data
- Users affected
- Actions taken
- Timeline of communication
- Post-incident recommendations

11. Staff Responsibilities

- All employees must report incidents immediately
- Only authorized personnel may handle breach response
- Confidentiality must be maintained at all times

12. Training

Staff must receive regular training on:

- Identifying threats
- Incident reporting procedures
- Data protection responsibilities

13. Review of the Plan

This Plan should be reviewed annually or after any significant breach.

14. Contact

LeadClosers d.o.o.

Gradiška 21, 10000 Zagreb, Croatia

Email: vladimir@leadclosers.eu