

Data Protection Impact Assessment (DPIA) — Momtivation App (LeadClosers d.o.o.)

Last updated: [insert date]

1. Introduction

This Data Protection Impact Assessment (DPIA) is conducted in accordance with GDPR Article 35 due to the processing of sensitive health data and integration with Apple Health / Recording API. The DPIA evaluates risks and defines safeguards to protect user data.

Data Controller:

LeadClosers d.o.o.

Gradiška 21, 10000 Zagreb, Croatia

Email: vladimir@leadclosers.eu

2. Description of Processing

Momtivation processes the following categories of data:

- Personal identification data: name, email, phone number
- Authentication data: encrypted password or social login identifiers
- Health data: weight, height, health issues, goals, postpartum details
- Apple Health / Recording API data: steps, distance, calories (read-only)
- Questionnaire responses
- Usage analytics
- Push notifications and marketing preferences
- User-generated content in the Feed

Processing purposes:

- Provide personalized workouts and nutrition suggestions
- Track health and fitness progress
- Enable social interaction via the Feed
- Improve app performance
- Maintain platform security

3. Legal Basis

- Contract performance (core functionality)
- Explicit consent (health data, Apple Health data, analytics, marketing)
- Legitimate interest (security, moderation, fraud prevention)

4. Assessment of Necessity and Proportionality

Data processing is necessary to:

- Tailor fitness and nutrition recommendations
- Track progress for user motivation
- Enable safe community interactions
- Improve user experience based on analytics

Proportionality safeguards:

- Minimal data collection
- No automated decisions with legal effect
- No sharing of personal data with affiliate partners
- No profiling beyond stated purposes

5. Risks to Data Subjects

Identified risks include:

- Unauthorized access to health data
- Leakage of Apple Health information
- Misuse of Feed content
- Exposure due to third-party processors (analytics, hosting)
- Data transfer risks to the U.S. under SCC
- Account compromise due to weak passwords or device access

Risk levels:

- Health data breach: High
- Apple Health data breach: Medium–High
- Analytics data misuse: Medium
- Feed exposure (user error): Medium
- Security breach: High

6. Measures to Mitigate Risks

Technical measures:

- Encryption in transit and at rest
- Strong authentication and hashing
- Segmented server infrastructure
- Logging and monitoring of unusual activity
- Regular software updates and vulnerability scans

Organizational measures:

- Staff training on data protection
- Access restricted to authorized personnel only

- Clear retention and deletion procedures
- DPIA annual review

User-facing measures:

- Transparent Privacy Policy and Health Data Disclosure
- Clear consent collection and withdrawal mechanisms
- Ability to delete account and all data
- In-app control over analytics and notifications

7. Residual Risk Evaluation

After mitigation measures:

- Overall risk level decreases to Medium.
- No remaining high-risk processing that requires consultation with the supervisory authority (AZOP).

8. Conclusion

The processing activities are compliant with GDPR requirements.

Risk is minimized through strong safeguards, explicit consent, and transparency measures.

9. Review Schedule

This DPIA must be reviewed every 12 months or sooner if:

- New features are added
- New sensitive data categories are introduced
- Significant changes to third-party processors occur

10. Contact

LeadClosers d.o.o.

Gradiška 21, 10000 Zagreb, Croatia

Email: vladimir@leadclosers.eu