

DPIA — Procjena učinka na zaštitu podataka (Momtivation)

DPIA (Data Protection Impact Assessment) provodi se zbog obrade zdravstvenih podataka, integracije s Apple Health / Recording API-jem i korištenja analitičkih alata. Dokument je izrađen u skladu s čl. 35. GDPR-a.

Voditelj obrade: LeadClosers d.o.o., Gradiška 21, 10000 Zagreb.

Kontakt: vladimir@leadclosers.eu

1. Opis obrade

Aplikacija obrađuje sljedeće kategorije podataka:

- osnovne korisničke podatke (ime, prezime, email, telefon),
- zdravstvene podatke (težina, visina, zdravstveni problemi, ciljevi),
- Apple Health / Recording API podatke (koraci, udaljenost, kalorije),
- korisnički sadržaj (objave, komentari),
- tehničke i analitičke podatke.

Svrhe obrade uključuju personalizaciju, komunikaciju, analitiku i sigurnost.

2. Procjena nužnosti i proporcionalnosti

Obrada zdravstvenih podataka nužna je za personalizirane preporuke. Obrada se temelji na izričitoj privoli. Obrađuju se samo podaci koje korisnik dobrovoljno unosi, a Apple Health podaci koriste se jedino za prikaz napretka.

3. Identifikacija rizika

Glavni rizici uključuju:

- neovlašteni pristup zdravstvenim podacima,
- curenje Apple Health podataka,
- objavu osjetljivih informacija u Feed-u,
- prijenos podataka izvan EU (SCC),
- kompromitaciju korisničkog računa.

4. Procjena rizika

Rizik = vjerojatnost × posljedice.

- Neovlašteni pristup zdravstvenim podacima → srednje-visok rizik.

- Apple Health podaci → srednji rizik.
- Feed objave → srednji rizik.
- Prijenos u SAD (SCC) → srednji rizik.
- Kompromitacija računa → visok rizik.

5. Mjere za smanjenje rizika

Tehničke mjere:

- enkripcija podataka u prijenosu i mirovanju,
- hashirane lozinke,
- ograničen pristup bazi podataka,
- sigurnosni logovi i monitoring,
- HTTPS enkripcija,
- segmentacija sustava.

Organizacijske mjere:

- politika zaštite podataka,
- redovita edukacija osoblja,
- procedure u slučaju povrede podataka,
- DPA ugovori sa svim pružateljima.

Mjere za korisnike:

- jednostavno povlačenje privola,
- jasne informacije o rizicima,
- brisanje računa i podataka u stvarnom vremenu.

6. Zaključak procjene

Uz primijenjene mjere, ukupna razina rizika procjenjuje se kao SREDNJA. Obrada se može nastaviti i nije potrebna konzultacija s nadzornim tijelom (AZOP).

7. Preporuke

Preporučuje se:

- redovita revizija DPIA (svakih 12 mjeseci),
- sigurnosna nadogradnja sustava,
- periodična obuka zaposlenika.