INCIDENT RESPONSE PLAN — Plan postupanja u slučaju povrede osobnih podataka

Ovaj dokument definira postupke koje LeadClosers d.o.o. mora poduzeti u slučaju povrede osobnih podataka, u skladu s člancima 33. i 34. GDPR-a. Plan se primjenjuje na sve obrade podataka povezane s Momtivation aplikacijom.

1. Definicija povrede podataka

Povreda osobnih podataka je sigurnosni incident koji dovodi do:

– gubitka podataka,

– uništenja,

– izmjene,

– neovlaštenog pristupa,

– neovlaštenog otkrivanja,

posebno zdravstvenih podataka ili Apple Health podataka.

2. Ciljevi incidentnog postupanja

– zaštititi korisnike,

– ograničiti štetu,

– spriječiti daljnje curenje podataka,

– osigurati usklađenost s GDPR člancima 33. i 34.

3. Faze upravljanja incidentom

Incident se rješava kroz sljedeće faze:

1) Identifikacija

2) Procjena

3) Zatvaranje sigurnosne rupe

4) Obavještavanje

5) Praćenje i prevencija

4. Identifikacija incidenta

Incident može otkriti:

– tehnički sustav (logovi, monitoring),

– zaposlenik,

– korisnik,

– partner (npr. procesor podataka).

Svi incidenti bilježe se u internu evidenciju povreda.

5. Procjena razine rizika

Procjenjuje se:

– vrsta podataka (posebne kategorije, Apple Health, identifikacijski),

– opseg povrede,

– broj pogođenih korisnika,

– je li vjerojatna materijalna šteta za korisnike.

Rizik može biti: nizak, srednji, visok.

6. Obavještavanje Agencije (AZOP)

Ako je vjerojatno da će povreda predstavljati rizik za prava korisnika, AZOP se obavještava u roku od 72 sata. Obavijest uključuje:

– opis povrede,

– kategorije i broj korisnika,

– posljedice povrede,

– mjere za smanjenje štete.

7. Obavještavanje korisnika

Ako povreda predstavlja VISOKI rizik, korisnici moraju biti obaviješteni bez odgađanja. Obavijest mora biti jasna i razumljiva te sadržavati:

– opis incidenta,

– moguće posljedice,

– preporučene mjere,

– kontakt voditelja obrade.

8. Privremene mjere

– blokiranje kompromitiranih računa,

– resetiranje lozinki,

– privremeno isključivanje pojedinih funkcija Aplikacije,

– ograničavanje pristupa sustavu administratorima.

9. Tehničke mjere nakon incidenta

– analiza ranjivosti,

– sigurnosna nadogradnja sustava,

– revizija logova,

– dodatno enkriptiranje podataka,

– izmjena pristupnih prava.

10. Dokumentiranje incidenta

Svaki incident mora biti dokumentiran i sadržavati:

– datum i vrijeme,

– izvor otkrivanja,

– opis povrede,

– pogođene korisnike,

– poduzete mjere,

– analizu učinkovitosti.

11. Obuka zaposlenika

Svi članovi tima moraju biti obučeni:

– kako prepoznati incident,

– kako ga prijaviti,

– kako postupati prema ovom Planu.

12. Redovita revizija plana

Plan se mora revidirati najmanje jednom godišnje ili nakon svake stvarne povrede.

13. Kontakt

Voditelj obrade:

LeadClosers d.o.o.

Email: vladimir@leadclosers.eu