Zásady GDPR

Ram Fintech s.r.o. · Návrh pro licenční řízení EMI

Vnitřní směrnice o ochraně osobních údajů

Společnost: Ram Fintech s.r.o.

Určeno pro: Zaměstnance, statutární orgány a kontrolní funkce

Verze: 1.0 (Regulatory Draft for ČNB)

Datum účinnosti: [Doplnit datum]

Garant dokumentu: Pověřenec pro ochranu osobních údajů (DPO)

1. Účel a rozsah směrnice

Tato směrnice stanovuje závazná pravidla pro nakládání s osobními údaji uvnitř společnosti Ram Fintech s.r.o. (dále jen „Společnost“). Směrnice je nedílnou součástí systému vnitřních zásad (Internal Control Framework) a je navržena tak, aby splňovala požadavky:

Obecného nařízení o ochraně osobních údajů (GDPR).

Zákona o platebním styku (ZPS) č. 370/2017 Sb.

AML zákona č. 253/2008 Sb.

Standardů kybernetické bezpečnosti (DORA, PCI DSS) popsaných v technické dokumentaci Společnosti.

2. Organizační struktura a odpovědnosti

2.1. Pověřenec pro ochranu osobních údajů (DPO)

Společnost jmenovala DPO, který:

Monitoruje soulad zpracování s právními předpisy.

Působí jako kontaktní místo pro Úřad pro ochranu osobních údajů (ÚOOÚ) a subjekty údajů.

Provádí pravidelná školení zaměstnanců.

2.2. AML Officer (Alena Bulachová)

Odpovídá za soulad zpracování údajů v rámci procesů KYC (Know Your Customer) a sledování sankčních seznamů. Úzká spolupráce s DPO je povinná při posuzování rizik (DPIA) u nových produktů.

2.3. IT a Security (Fixosoft / Internal IT)

Odpovídá za technické zabezpečení dat v prostředí AWS, správu přístupových práv a monitoring logů.

3. Klasifikace dat a technická infrastruktura

V souladu s dokumentem Internal Control and ICT Systems Description:

Úložiště dat: Primární region AWS Frankfurt (eu-central-1), záložní region AWS Ireland (eu-west-1).

Zabezpečení: Všechna produkční data jsou šifrována (AES-256). Přístup k databázi je povolen pouze přes šifrované VPN spojení s vícefaktorovou autentizací (MFA).

Kategorizace: Osobní údaje klientů jsou klasifikovány jako "Důvěrné" (Confidential) a podléhají nejpřísnějšímu režimu ochrany.

4. Pravidla přístupu k datům (Access Control)

Společnost uplatňuje princip „Need-to-know“ a „Least privilege“:

Zákaznická podpora: Přístup k základním identifikačním údajům pouze v rozsahu nezbytném pro odbavení požadavku.

Compliance/AML tým: Přístup k transakční historii a identifikačním dokladům pro účely hlášení FAÚ.

Administrátoři: Přístup k surovým datům je logován a pravidelně revidován (CIS Hardened Reports).

5. Správa dokumentace a retenční lhůty

V souladu s AML programem Společnosti:

Složka klienta (KYC): Musí obsahovat kopie dokladů, záznam o kontrole v sankčních seznamech a PEP status.

Archivace: Dokumenty jsou uchovávány po dobu 10 let od ukončení obchodního vztahu. Po uplynutí této lhůty musí být data nevratně smazána nebo anonymizována, pokud neexistuje jiný zákonný důvod pro jejich uchování.

6. Postup při porušení zabezpečení (Data Breach Protocol)

V případě detekce úniku dat nebo neoprávněného přístupu (např. narušení bezpečnosti AWS nebo útok na koncové zařízení):

Detekce: Hlášení incidentu na [dpo@ram-fintech.com] a IT Security týmu.

Posouzení: DPO vyhodnotí riziko pro práva a svobody subjektů údajů.

Oznámení ÚOOÚ: Pokud hrozí riziko, DPO podá oznámení Úřadu do 72 hodin.

Informování klientů: Pokud hrozí vysoké riziko, jsou klienti informováni bez zbytečného odkladu (e-mailem nebo v aplikaci).

Dokumentace: Každý incident musí být zapsán do „Knihy incidentů“ včetně přijatých nápravných opatření.

7. Práva subjektů údajů – interní vyřizování

Žádost o přístup k údajům musí být vyřízena do 30 dnů.

Žádost o výmaz: Před smazáním musí Compliance oddělení potvrdit, že již neplatí povinnost uchovávat data dle AML zákona.

8. Školení a mlčenlivost

Každý zaměstnanec podepisuje dohodu o mlčenlivosti (NDA) jako součást pracovní smlouvy.

Školení na ochranu osobních údajů a kybernetickou bezpečnost probíhá minimálně 1x ročně.

9. Kontrola a sankce

Dodržování této směrnice je předmětem interního auditu. Porušení pravidel může být klasifikováno jako závažné porušení pracovních povinností s následky dle zákoníku práce.

Schváleno vedením společnosti Ram Fintech s.r.o.