מדיניות GDPR

EMI טיוטה להליך רישוי · Ram Fintech s.r.o.

הנחיות פנימיות בנושא הגנת מידע אישי

חברה: Ram Fintech s.r.o.

מיועד ל: עובדים, גופים סטטוטוריים ותפקידי בקרה

גרסה: 1.0 (טיוטת תקנות עבור ČNB)

תאריך כניסה לתוקף: [יש להוסיף תאריך]

אחראי על המסמך: הממונה על הגנת המידע (DPO)

1. מטרת ההנחיה והיקפה

הנחיה זו קובעת כללים מחייבים לטיפול במידע אישי בתוך חברת Ram Fintech s.r.o. (להלן "החברה"). הנחיה זו מהווה חלק בלתי נפרד ממערכת העקרונות הפנימיים (Internal Control Framework) והיא נועדה לעמוד בדרישות:

התקנה הכללית להגנה על מידע אישי (GDPR).

חוק התשלומים (ZPS) מס' 370/2017

חוק AML מס' 253/2008

תקני אבטחת סייבר (DORA, PCI DSS) המתוארים בתיעוד הטכני של החברה.

2. מבנה ארגוני ותחומי אחריות

2.1. ממונה על הגנת נתונים אישיים (DPO)

החברה מינתה ממונה על הגנת נתונים (DPO) אשר:

מפקח על עמידת הטיפול בנתונים בדרישות החוק.

משמש כנקודת קשר בין הרשות להגנת מידע אישי (ÚOOÚ) לבין בעלי המידע.

מקיים הדרכות קבועות לעובדים.

2.2. אחראית למאבק בהלבנת הון (אלנה בולאכובה)

הוא אחראי על עמידת עיבוד הנתונים בתהליכי KYC (Know Your Customer) ובבדיקת רשימות הסנקציות. שיתוף פעולה הדוק עם הממונה על הגנת המידע (DPO) הוא חובה בעת ביצוע הערכת סיכונים (DPIA) למוצרים חדשים.

2.3. אבטחת מידע (Fixosoft / מחלקת ה-IT הפנימית)

אחראי על האבטחה הטכנית של הנתונים בסביבת AWS, ניהול זכויות הגישה וניטור יומנים.

3. סיווג נתונים ותשתית טכנית

בהתאם למסמך תיאור מערכות הבקרה הפנימית וה-ICT:

אחסון נתונים: אזור ראשי של AWS בפרנקפורט (eu-central-1), אזור גיבוי של AWS באירלנד (eu-west-1).

אבטחה: כל נתוני הייצור מוצפנים (AES-256). הגישה למסד הנתונים מותרת רק באמצעות חיבור VPN מוצפן עם אימות

רב-גורמי (MFA).

סיווג: נתוני הלקוחות מסווגים כ"סודיים" (Confidential) וכפופים למדיניות האבטחה המחמירה ביותר.

4. כללי גישה לנתונים (בקרת גישה)

החברה מיישמת את עקרונות "הצורך לדעת" ו"הרשאות מינימליות":

שירות לקוחות: גישה לפרטי זיהוי בסיסיים רק במידה הנדרשת לטיפול בבקשה.

צוות ציות/AML: גישה להיסטוריית העסקאות ולמסמכי הזיהוי לצורך דיווח לרשות למאבק בהלבנת הון (FAÚ).

מנהלים: הגישה לנתונים הגולמיים מתועדת ונבדקת באופן קבוע (דוחות CIS Hardened).

5. ניהול תיעוד ותקופות שמירה

בהתאם לתוכנית למניעת הלבנת הון של החברה:

תיק הלקוח (KYC): חייב לכלול עותקי מסמכים, תיעוד של בדיקת רשימות הסנקציות וסטטוס PEP.

ארכוב: המסמכים נשמרים למשך 10 שנים ממועד סיום הקשר העסקי. בתום תקופה זו, יש למחוק את הנתונים באופן בלתי הפיך או להפוך אותם לאנונימיים, אלא אם קיימת עילה חוקית אחרת לשמירתם.

6. נוהל במקרה של פרצת אבטחה (Data Breach Protocol)

במקרה של זיהוי דליפת נתונים או גישה בלתי מורשית (למשל, פרצת אבטחה ב-AWS או מתקפה על מכשיר קצה):

איתור: דיווח על האירוע לכתובת [dpo@ram-fintech.com] ולצוות אבטחת ה-IT.

הערכה: הממונה על הגנת המידע יעריך את הסיכון לזכויותיהם ולחירויותיהם של נושאי המידע.

הודעה לרשות להגנת מידע: במקרה של סיכון, ממונה הגנת המידע יגיש הודעה לרשות בתוך 72 שעות.

יידוע הלקוחות: במקרה של סיכון גבוה, הלקוחות יקבלו הודעה ללא דיחוי (בדוא"ל או באפליקציה).

תיעוד: יש לתעד כל אירוע ב"ספר האירועים", כולל אמצעי התיקון שננקטו.

7. זכויות בעלי המידע – טיפול פנימי

יש לטפל בבקשה לקבלת גישה לנתונים בתוך 30 ימים.

בקשה למחיקה: לפני המחיקה, מחלקת הציות חייבת לאשר כי כבר לא חלה חובה לשמור את הנתונים בהתאם לחוק למניעת הלבנת הון.

8. הכשרה וסודיות

כל עובד חותם על הסכם סודיות (NDA) כחלק מחוזה העבודה.

ההדרכה בנושא הגנה על מידע אישי ואבטחת סייבר מתקיימת לפחות פעם בשנה.

9. פיקוח וענישה

הקפדה על הנחיות אלה היא נושא לביקורת פנימית. הפרת הכללים עשויה להיחשב כהפרה חמורה של חובות העבודה, עם השלכות בהתאם לחוק העבודה.

אושר על ידי הנהלת חברת Ram Fintech s.r.o.