מדיניות הגנת הפרטיות

1. רקע

1.1 הגנה על פרטיות המידע היא ערך יסוד בחברה. מדיניות זו מבטיחה כי מידע אישי הנאסף, נשמר ומעובד בידי החברה מטופל באופן חוקי, הוגן ומאובטח, בהתאם לדין החל – לרבות חוק הגנת הפרטיות, תקנות הגנת הפרטיות (אבטחת מידע), ותיקון 13 שנכנס לתוקף באוגוסט 2025.

2. מטרות

2.1 להבטיח עיבוד מידע אישי באופן חוקי, הוגן ושקוף.
2.2 להגדיר אחריות עובדים ומנהלים בנוגע להגנה על מידע אישי.
2.3 לעמוד בדרישות הרגולציה לצורך רישוי גוף פיננסי.

3. הגדרות

3.1 "הארגון" – מקסימוס קרדיט בע"מ.
3.2 "מידע אישי" - כל מידע המזהה אדם או שניתן לזהותו ממנו, לרבות שם, ת.ז., פרטי קשר, כתובת IP, מידע בריאותי וכו.'
3.3 מאגר מידע - כמשמעותו בחוק הגנת הפרטיות.
3.4 בעל מידע - האדם שהמידע נוגע אליו.
3.5 עיבוד מידע - כל פעולה במידע, כולל איסוף, אחסון, גישה, העברה או מחיקה.
3.6 מידע רגיש - כולל נתוני בריאות, אמצעי תשלום, מיקום וכיו"ב.
3.7 קבלן עיבוד (Processor) - גורם המעבד מידע עבור החברה.
3.8 אנונימיזציה – עיבוד המונע זיהוי אדם באופן בלתי־הפיך.
3.9 פסאודונימיזציה – הפרדת מזהים ישירים ושמירת מפתח/מיפוי בנפרד.
3.10 Tokenization - המרת מזהים רגישים לאסימונים בלתי־שמישים לצמצום סיכון.
3.11 RoPA - רישום פעילויות עיבוד.
3.12 DPIA/PIA - הערכת השפעת פרטיות לעיבוד/שינוי בעל סיכון גבוה.
3.13 DSR – בקשת בעל מידע (Data Subject Request).

4. תחולה

4.1 המדיניות חלה על כלל עובדי החברה, קבלני משנה, ספקים וכל גורם המעבד מידע אישי עבור החברה; ועל כלל הסביבות (לרבות ענן וספקי צד שלישי) בהן מעובד המידע.

5. אחריות

5.1 מנכ"לית – אחריות כוללת על יישום המדיניות, מעקב אחר תוכנית אבטחת מידע וביקורות הגנת הפרטיות.
5.2 ממונה אבטחת מידע – כתיבה ועדכון נהלי אבטחת מידע ובקרה על יישומם

6. שיטה

6.1 עקרונות הטיפול במידע אישי

6.1.1 מידע אישי ייאסף רק למטרה לגיטימית וברורה, בכמות מינימלית הדרושה.
6.1.2 כל עיבוד מידע יתבצע על בסיס חוקי, כולל קבלת הסכמה, חוזה, חובה חוקית או אינטרס לגיטימי.
6.1.3 תישמר שקיפות מול בעלי מידע: מדיניות פרטיות זמינה, הודעות איסוף ברורות.
6.1.4 מידע יישמר רק לפרק זמן נדרש למטרות שהוגדרו.
6.1.5 יינקטו אמצעים מתאימים לשמירה על אבטחת המידע: בקרות גישה, הצפנה, מנגנון אימות דו־שלבי (2FA) לחשבונות קריטיים.
6.1.6 דיוק ועדכון: החברה תפעל לשמירת דיוק המידע האישי ולעדכונו או תיקונו ללא דיחוי סביר.
6.1.7 Privacy by Design & Default: שילוב עקרונות פרטיות כבר בתכנון מערכות ותהליכים והגדרת ברירות מחדל מצמצמות מידע.

6.2 זכויות נושאי מידע

6.2.1 זכות לעיון במידע.
6.2.2 זכות לתיקון.
6.2.3 זכות למחיקה.
6.2.4 זכות להגביל עיבוד.

6.3 שימור נתונים ולוגים (Retention)

6.3.1 שמירת לוגים תנוהל על ידי הספקים הרלוונטיים.
6.3.2 ככל האפשר, לוגים של גישה ופעילות במערכות המידע יישמרו ל-24 חודשים לפחות.

6.4 עיבוד אצל ספקים והעברות מידע

6.4.1 התקשרות עם קבלני עיבוד תיעשה בהסכם הכולל התייחסות להיבטי סודיות, אבטחת מידע ופרטיות.
6.4.2 העברות מידע מחוץ לישראל יבוצעו בהתאם לדין ובהתקיים אמצעי הגנה הולמים (לרבות מנגנונים חוזיים סטנדרטיים).
6.4.3 ספקים קריטיים יוערכו בסיכון וייבדקו תקופתית (Due Diligence ובקרות אבטחה).
6.4.4 העברות מחוץ לישראל יתבצעו רק בהתקיים תנאי העברה חוקיים ובהסכמים מתאימים (לרבות סעיפים חוזיים תקניים, התחייבויות סודיות ובקרות אבטחה).

6.5 דיווח על הפרת פרטיות

במקרה של "פגיעה חמורה בפרטיות", החברה תפעל לפי הדין, לרבות דיווח לרשות להגנת הפרטיות ויידוע נושאי מידע, לצד ניהול האירוע לפי "נוהל תגובה ודיווח לאירוע סייבר".