

# מדיניות אבטחת מידע

עדכון אחרון: 27 יוני 2023

Nipendo Ltd. (להלן "החברה" או "אנחנו") מחויבת לשקיפות בהקשר של אמצעי האבטחה שאנו מיישמים כדי לאבטח ולהגן על מידע אישי, כמוגדר במסגרת חוק הגנת הנתונים החל, כולל וללא הגבלה, חוק הגנת הפרטיות, התשמ"א – 1981, החל בישראל וכל התקנות הנובעות מנו.

מדיניות אבטחת המידע מפרטת את נהלי האבטחה, את האמצעים הטכניים ואת הנהלים הארגוניים של החברה.

בחלק מתהליך הציות שלנו בהקשר של הגנת הנתונים, יישמנו אמצעי אבטחה טכניים, פיזיים ומנהליים שנועדו להגן על מידע אישי, כולל ציות לתקנים IOS 27001 וכן SOC 2 Type II.

## בקרת גישה פיזית

החברה מוודאת הגנה על הגישה הפיזית לשרתים שבהם מאוחסן המידע האישי. הנתונים המעובדים על ידי החברה מאוחסנים בחוות השרתים הפרטיות של החברה. בנוסף, החברה מאבטחת את הגישה הפיזית אל משרדיה כדי לוודא שרק גורמים מורשים כגון עובדים או צדדים שלישיים מורשים (צוות תחזוקה, מבקרים מורשים וכו') מקבלים גישה אל משרדי החברה.

## בקרת מערכת

הגישה את מסד הנתונים של החברה מוגבלת לעובדים מאושרים בלבד, כולל באמצעות הבטחת אמצעי אבטחה הקשורים לגישה מרחוק ויכולות מחשוב אלחוטיות. אנו מקצים לעובדים סיסמאות פרטיות המאפשרות גישה או שימוש בהקשר של מידע אישי, בהתאם לתפקידם ורק בהיקף הדרוש לצורך מילוי תפקידם. החברה מנטרת גישה של משתמשים לנתונים ושל הסיסמאות המשמשות כדי לקבל גישה כגון זו.

## בקרת גישה לנתונים

החברה מוודאת שגישה למידע אישי מוגבל לעובדים מורשים בלבד כדי למנוע גישה, שינוי, העתקה, שימוש, העברה או מחיקה של מידע אישי ללא הרשאה ספציפית. גישה למידע אישי, כמו גם כל פעולה הקשורה בשימוש במידע אישי, מחייבת שם משתמש וסיסמה, המשתנה באופן שגרתי ומוצפנת באופן מלא. כל עובד יכול לבצע פעולות מסוימות בהתאם להרשאות שהוענקו לו על ידי החברה. הגישה של כל אחד מהעובדים נרשמת וכל גישה בלתי מורשית מדווחת באופן אוטומטי. בנוסף, החברה מבצעת ביקורות שוטפות כדי לקבוע אם הרשאות הגישה שהוענקו לעובדים עדיין נדרשות. עובדים מורשים יכולים קבל גישה רק למידע אישי שצוין בפרופיל האישי שלהם. בנוסף, החברה מבטלת את הרשאות הגישה בעת עזיבה או פיטורין של עובד.

## אבטחה ארגונית ותפעולית

החברה משקיעה מאמצים ומשאבים רבים כדי להבטיח תאימות לנוהלי האבטחה של החברה, כולל קיום הדרכות שוטפות לעובדים. בנוסף, החברה מיישמת אמצעי הגנה ישימים כדי לאבטח את החומרה והתוכנה, כולל חומות אש ופתרונות אנטי-וירוס שנועדו להתגונן בפני מתקפות של תוכנות זדוניות.

## בקרת העברת נתונים

אנו מגנים כל מעבר של מידע אישי בין הלקוח ושרתי החברה באמצעות יישום אמצעי הצפנה, כולל הצפנה של המידע האישי לפני העברתו. בנוסף, כשהדבר ישים, החברה חותמת על הסכמי עיבוד נתונים, בהתאם לחוקים החלים.

## בקרת זמינות

שרתי החברה כוללים הליך גיבוי אוטומטי שמתקיים על בסיס יומי.

## **החזקת נתונים**

החברה מחזיקה במידע אישי למשך פרקי הזמן הנדרשים לצורך אספקת השירותים או בהתאם לנדרש במסגרת החוקים החלים. כל נשוא נתונים יכול לבקש מחיקה של נתונים, בכפוף למגבלות מסימות, כמפורט בהודעה בדבר זכויות של נשוא נתונים של החברה.

## **בקרת משימות**

כל עובדי החברה נדרשים לקיים את תנאי הסכם ההעסקה, הכולל, כשהדבר ישים, סעיפי סודיות, כמו גם סעיפים המחייבים את העובדים לציית לנהלי אבטחת הנתונים הישימים. בנוסף, כל עובדינו עוברים תהליך סינון בהתאם לדרישות החלות. במקרה של הפרת התחייבות של עובד או אי ציות לכללי המדיניות של החברה על ידי עובד כלשהו, החברה תנקוט בפעולות התיקון המתאימות.

## **עדכונים להליך זה**

פעם בשנה, נבצע הערכה כדי לקבוע אם יש צורך לעדכן הליך זה, כולל באמצעות בחינה אם חלו שינויים מהותיים כלשהם במערכות מסדי הנתונים או בנהלי עיבוד המידע שלנו ואף נבדוק אם קיימים סיכונים טכנולוגיים חדשים בהקשר של מערכות מסדי הנתונים שלנו.