

נספח מיקור חוץ של מידע אישי

נספח מיקור החוץ של מידע אישי זה הינו חלק בלתי נפרד מתנאי השימוש של חשבונות ירוקה בע"מ (להלן: "החברה") הזמנים [כאן](#) (להלן: "תנאי השימוש"). בהסכמתך לתנאי השימוש הנך (להלן: "הלקוח") מאשר את תנאי נספח זה.

הואיל ובמסגרת מתן השירותים בהתאם לתנאי השימוש, החברה עשויה לעבד מידע אישי (כהגדרתו (להלן) עבור הלקוח, בהתאם לעמידה בדרישות החוק והוראות הלקוח כפי שבאות לידי ביטוי בתנאי השימוש וכן בפעולות ובקונפיגורציות מורשות במערכת;

והואיל ובמהלך מתן השירותים תבצע החברה פעולות ותהליכים במידע, כהגדרתו בחוק הגנת הפרטיות, התשמ"א – 1981 (להלן: "החוק"), של הלקוח או עבורו (להלן: "המידע");

לפיכך, הוצהר, הותנה והוסכם בין הצדדים כדלהלן:

1. **כללי**- הוראות נספח זה גוברות על הוראות תנאי השימוש. החברה עשויה לעדכן את הנספח, כל עוד שעדכון או שינוי כאמור לא יפגע בהתחייבויות החברה לפי נספח זה, ברמת הגנת הפרטיות או ברמת אבטחת המידע ביחס למידע של הלקוח וזאת ככל שמתאפשר באופן סביר.

2. **מידע פיננסי**- מובהר כי בכל הקשור למידע פיננסי, החברה מחזיקה ברישיון נותן שירות מידע פיננסי בהתאם לחוק שירות מידע פיננסי, תשפ"ב-2021, ופועלת בהתאם להוראות החוק. החברה מפוקחת בעניין זה תחת רשות ניירות ערך.

3. **עיבוד מידע על ידי החברה**- בכפוף לאמור בתנאי השימוש, החברה מתחייבת כי היא לא תעביר או תגלה את המידע לכל צד ג', מלבד נותני שירותים של החברה, אלא בהסכמת הלקוח. גישה למידע תינתן אך ורק למי אשר תפקידו מחייב גישה למידע על פי תנאי השימוש ונספח זה, ואשר מחויב על פי דין או הסכם לשמור על פרטיות המידע ואשר מחויב למלא אחר תנאי נספח זה ו/או תנאים דומים. רשימת משרות אצל החברה וסוגי אנשי צוות שתהיה להם גישה למידע אישי, וכן רמות הגישה המותרת רשומים ב**תוספת 1** להלן.

4. **שמירה והחזרה של מידע**- בכפוף להוראות הדין ולהוראות תנאי השימוש, החברה תשמור את המידע שנאסף עבור ו/או בשם הלקוח כל עוד יש צורך בכך על מנת להגשים את המטרות שלשמן הועבר לחברה. החברה תחזיר, תמחק או תבער ללא אפשרות אחזור את כל המידע מיד לאחר בקשת הלקוח בכתב או בסיום ההתקשרות ו/או נספח זה, לפי המוקדם ביניהם. על אף האמור לעיל, החברה רשאית לשמור עותק מהמידע לצורך התגוננות בפני הליכים משפטיים ו/או בהתאם להוראות כל דין.

5. **זכויות עיון ותיקון של נושאי המידע**- החברה תסייע ללקוח למלא אחר דרישות הדין החל בנושא עיון ותיקון של המידע על ידי נושאי המידע. אם נושא המידע ו/או נציגו המורשה יגיש בקשה בכתב לחברה לעיין במידע שלו, החברה: (א) תודיע לנושא המידע אם החברה מעבדת את המידע שלו, ולא תמסור לו כל מידע נוסף (למעט האמור בס"ק (ב) להלן); (ב) תמסור לנושא המידע את שם הלקוח ופרטי התקשרות לפניות נוספות; ו-(ג) תודיע ללקוח בכתב אודות הפנייה בצירוף הפרטים הרלוונטיים. היה ויתברר כי המידע אינו מדויק, אינו שלם או אינו עדכני, תבצע החברה את התיקונים הנדרשים, כפי שיורה לה הלקוח ותודיע ללקוח בכתב על תיקון המידע לאחר שיבוצע.

6. **אבטחת המידע**- החברה תיישם אמצעי אבטחה בהתאם להוראות החוק. החברה תודיע ללקוח בכתב על כל פגיעה באבטחת המידע המשפיעה על המידע המעובד על ידי החברה עבור או בשם הלקוח תוך זמן סביר. החברה מפרטת ומיישמת אמצעי אבטחת מידע טכניים וארגוניים מתאימים, לרבות:

- **הצפנה:** הצפנת מידע במעבר (Data in Transit) באמצעות TLS 1.2 ומעלה, והצפנה במנוחה (Data at Rest) באחסון ב-VPN.

- **הרשאות ובקרה:** ניהול גישה על בסיס Need-to-Know, אימות רב-שלבי (MFA), והפרדה לוגית מלאה של מידע הלקוח.

- **ניטור ואירועים:** תיעוד יומני רישום (Logs), ניטור, ודיווח ללקוח על אירוע אבטחה מהותי.

- **יובהר,** כי החברה מתחייבת לפעול בהתאם לדין במקרה של אירוע אבטחה חמור כפי שמוגדר בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017.

7. **דיווח**- החברה תמציא אחת לשנה ו/או לבקשתו הסבירה של הלקוח אישור על פיו קיימה חובותיה בהתאם לנספח זה, לרבות באמצעות אישור על עמידתה בתקן אבטחת מידע בין-לאומי (ISO).

8. **אחסון המידע והעברתו מחוץ לישראל** - אחסון המידע ועיבודו אצל ספקי משנה מבוצעים בישראל ו/או אצל ספקי שירותי ענן מובילים כדוגמ. (AWS) העברת מידע מחוץ לישראל תתבצע בהתאם להוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001, לרבות למדינות העומדות בGDPR. רשימת ספקי משנה מפורטת להלן בנספח 2, והעברת המידע אליהם מבוצעת בהתאם לדין.

9. **סיום ההתקשרות והדין החל** - החובות של החברה לפי נספח זה יחולו כל עוד היא מספקת את השירותים ללקוח ו/או יש לה גישה למידע. למען הסר ספק, חובות אלה לא יחולו על מידע סטטיסטי לא מזהה. הצדדים מסכימים בזאת כי הדין החל על נספח זה הינו הדין הישראלי. כל סכסוך הנובע מנספח זה או בקשר עימו יידון על-ידי בתי המשפט המוסמכים בתל אביב-יפו בלבד.

תוספת 1

פרטי עיבוד המידע

• מחלקת התמיכה - Editor • מחלקת דטה - Viewer • מחלקת מרקטינג - Viewer • צוות טכני - Editor • מחלקת פרודקט - Viewer • מחלקת כספים ואופרציה - Viewer	תפקיד אנשי צוות של החברה שתהיה להם גישה למידע, וכן רמות הגישה המותרות
מידע על עובדיו, ספקיו ולקוחותיו של הלקוח, לרבות שמות, פרטי קשר ומידע פיננסי.	סוגי מידע שיעובדו על ידי החברה
מתן השירותים על פי תנאי השימוש.	מטרת עיבוד המידע
עיבוד מידע למתן השירותים על פי תנאי השימוש וכל עיבוד אחר בהתאם לתנאי השימוש.	סוגי העיבוד המותרים
בהתאם לבחירת הלקוח ועל פי האינטגרציות הקיימות במערכות החברה.	מערכות להן תינתן גישה לחברה
שיר קמפוס מרטינוב – DPO privacy@morning.co	איש/ אשת הקשר של החברה לכל עניין הקשור לנספח זה

	Information Security Policy
Date of Version	Aug 2026 23

Information Security Policy

1. Introduction

This document constitutes the Company's **Information Security Policy**. It is aligned with the organization's ISMS and PIMS frameworks (ISO 27001, ISO 27701) and applies to all employees, contractors, and third parties who have access to information systems and assets.

2. Scope and Objectives

:This policy applies to all company information assets and databases, including

- Personal data of customers, employees, and suppliers
- Internal business, financial, and technological information
- Core systems, development and production environments, and cloud infrastructure (AWS)

Objectives

- Ensure the **confidentiality, integrity, and availability (CIA)** of data
- Protect information from unauthorized access, alteration, or loss
- Comply with legal, regulatory, and contractual requirements

Roles and Responsibilities .3

- **Senior Management** – Approves the policy, allocates resources, and ensures enforcement
- **Chief Information Security Officer (CISO)** – Maintains and updates this policy, oversees compliance, manages risk assessments, and reports to management
- **IT Manager** – Implements and operates technical and security controls
- **All Employees and Users** – Must comply with this policy, protect data, and immediately report any suspected security incident

Security Measures .4

Access Control 4.1

- (Users are granted the minimum privileges required (least privilege principle
- (Strong authentication enforced (complex passwords, MFA
- Quarterly access rights reviews; immediate revocation upon employee termination

Encryption 4.2

- **Data at Rest** – Encrypted using AES-256, FileVault, TDE, or equivalent
- **Data in Transit** – Encrypted using TLS 1.2+ or VPN

Systems and Endpoints 4.3

- Endpoint protection (antivirus/EDR) installed and updated
- Automated OS and software patching
- SIEM/log monitoring for anomalies and suspicious activities

Backup and Recovery 4.4

- Daily backups for production and development environments

- .Periodic restoration testing
- .(Documented **DRP** (Disaster Recovery Plan) and **BCP** (Business Continuity Plan)

Physical and Environmental Security 4.5

- .Controlled access to secured facilities
- .Enforced **Clear Desk / Clear Screen** policy
- .Prohibition of removable media unless formally authorized

Risk Management .5

- .Annual risk assessments conducted according to **ISO 31000**
- .Risks are evaluated based on **likelihood × impact**
- .Treatment strategies: Accept, Mitigate, Transfer, or Avoid
- .(Documented in the Risk Treatment Plan (RTP) and Statement of Applicability (SoA)

Incident Management .6

- .All employees must report suspected security incidents immediately
- The **CIRT (Computer Incident Response Team)**, led by the CISO and IT Manager, is responsible for containment, investigation, and remediation
- .Lessons learned are documented and integrated into updated controls
- Notification obligations: report material data breaches to the **Israeli Privacy Protection Authority** and, when applicable, affected customers

Awareness and Training .7

- Mandatory information security and privacy training for all employees at onboarding and annually thereafter

- Periodic awareness campaigns and simulated exercises (e.g., phishing tests, BCP drills).

8. Monitoring, Review, and Improvement

- Internal audits at least annually.
- Management reviews on a quarterly basis.
- Continuous improvement process, adapting to regulatory changes, technological developments, and emerging threats.

9. Commitment Statement

The Company is committed to protecting personal data and sensitive information, minimizing risks, and complying with Israeli law and global best practices in information security.

נספח 2 - רשימת ספקי משנה :

AWS - <https://aws.amazon.com/contact-us/compliance-support/> אחסון ועיבוד נתונים בתשתית הענן לצורך אספקה שוטפת, אבטחה ותפעול של המערכת.

Intercom - <https://www.intercom.com/help/en/> מתן מענה ותמיכה טכנית. העברת מידע וגישה אליו יתבצעו אך ורק ביוזמת הלקוח בעת פנייה מצידו, וביחס למידע שהלקוח יבחר למסור מיוזמתו במסגרת התקשורת.

Gemina - <https://www.gemina.co.il/contact> גישה לקריאה ופענוח של פרטי הוצאות (OCR). הגישה תתאפשר ככל והלקוח יבחר להפעיל ולנצל פיצ'ר זה, ומוגבלת לפרטי המסמך הנדרשים לעיבוד בלבד.

ספקי בינה מלאכותית OpenAI, Anthropic, ו-Google - עיבוד נתונים קיימים במערכת לפי בקשה יזומה של הלקוח, ולצורך מתן השירות המבוקש הספציפי בלבד ולפי נתונים שקיימים במערכת. הנתונים לא יישמשו לאימון מודלים של הספק.