



יעקב עוז ושות'

פרטיות • אבטחת מידע • סייבר

הערכה המשפטית

בעלת תפקיד יקר.ה,

הערכה המשפטית הינה תוצר "נושם", לכבוד יהא לנו לקבל ממך כל הארה, הערה ובקשה לתוספת מקצועית החסרה בערכה, לדעתך.

חוק הגנת הפרטיות ותקנותיו עברו, עוברים ויעברו בעת הקרובה שינויים רבים, ביניהם הרחבת סמכויות האכיפה של הרשות להגנת הפרטיות והתאמת הדין הישראלי לדיני הגנת הפרטיות בעולם.

המשפט והרגולציה מנסות להתאים עצמן לקצב התקדמות הטכנולוגיה והתאמה זו דורשת מעורבות של בעלי תפקיד כמוך וכמונו מתחום המשפט והטכנולוגיה.

לדעתנו, חוק הסייבר שחקיקתו לא צלחה עד כה יחוקק בעתיד הקרוב. כל זאת בנוסף להנחיות רגולטוריות, דרישות חוזיות וציפיות הציבור לשמירה על פרטיותו, מחייבים אותנו העוסקים במלאכה לפעול באופן אחראי תוך הפעלת שיקול דעת למימוש מטרות הארגון אליו אנו משתייכים מחד גיסא, והאינטרס הציבורי מאידך גיסא.

המידע המוצג במאמר זה הוא מידע כללי בלבד, ואין בו כדי להוות ייעוץ ו/או חוות דעת משפטית. המחברים אינם נושאים באחריות כלשהי כלפי הקוראים, ואלה נדרשים לקבל עצה מקצועית לפני כל פעולה המסתמכת על הדברים האמורים.

בברכה,

עו"ד שמעון ריינר

עו"ד יעקב עוז

המסגרת הנורמטיבית הכללית

להלן יפורטו החוקים, התקנות והצו החלים בקשר עם הגנת הפרטיות
ואבטחת מידע:

חוק יסוד: כבוד האדם וחירותו

חוק הגנת הפרטיות, התשמ"א - 1981 (להלן: החוק)

תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-

1981

צו הגנת הפרטיות (קביעת גופים ציבוריים), תשמ"ו - 1986

תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים),

תשמ"ו-1986

תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001

תקנות העבירות המינהליות (קנס מינהלי – הגנת הפרטיות), תשס"ד-2004

תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז – 2017 (להלן: התקנות)

תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג

2023 -

מסגרת נורמטיבית ספציפית

חוק הגנת הפרטיות, תשמ"א-1981

https://www.nevo.co.il/law_html/law00/71631.htm

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

https://www.nevo.co.il/law_html/law00/144811.htm

חוק המחשבים, תשנ"ה-1995

https://www.nevo.co.il/law_html/law00/72393.htm

בעלי תפקידים

בעל מאגר- יוגדר בתיקון 14

מנהל מאגר- מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה;

מחזיק, לעניין מאגר מידע- מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש;

ממונה על אבטחה- [כמשמעותו בסעיף 17 ב לחוק](#);

ממונה על אבטחת מידע- [כמשמעותו בתקנה 3 לתקנות הגנת הפרטיות\(אבטחת מידע\), התשע"ז-2017](#)

ממונה הגנת פרטיות DPO-

גילוי	דעת	מאת	הרשות	להגנת	פרטיות-
https://www.gov.il/BlobFolder/dynamiccollectorresultitem/doc_56/he/dpo_doc.pdf					

מדריך לארגונים :מינוי ממונה הגנה על הפרטיות בארגון ותפקידי-
https://www.gov.il/BlobFolder/dynamiccollectorresultitem/doc_56/he/dpo_kit.pdf

התנאים המחויבים כדי להיות DPO של חברה הנותנת שירותים לחברות אירופאיות ב-EU

מינוי DPO, תפקידו והדרישות למינויו נגזרות מסעי' 37 עד 39 ל-GDPR.

הבסיס לשאלת הנדרש למינוי DPO כמפורט בכותרת, הינו תקנות ה-GDPR, המלצות הרשות להגנת פרטיות בישראל והמלצות הרשות הצרפתית לאבטחת מידע ופרטיות (CNIL)

קציני הגנת נתונים - (DPO) מי אחראי בארגון שלך על אכיפת הרגולציה?

ה-GDPR יצר תפקיד חדש שלא היה קיים קודם: קצין הגנת נתונים נקרא גם DPO. מטרתו של ה-DPO הוא לוודא שיש הלימה לרגולציה והוא נדרש באחד מן המצבים הבאים –

- כאשר עיבוד הנתונים האישיים נעשה על ידי גופים ציבוריים.
 - כאשר פעילות הליבה של הארגון מורכבת מפעולות ניטור קבוע ושיטתי של Big Data נפח הנתונים, מספר נושאי הנתונים, משך העיבוד, ההיקף הגיאוגרפי שלו וכד'.
 - כאשר קיים עיבוד של נתונים רגישים במיוחד (גזע, דת, חיי מין, פלילים וכד').
- ה-DPO יכול למלא תפקיד אחר בארגון, אך בשביל למנוע ניגוד עניינים, הוא לא יכול להיות המנכ"ל, סמנכ"ל הכספים, המנכ"ר, מנהל השיווק או מנהל ה-HR.

יש חשיבות עליונה להימצאו של DPO בארגון, אך ניתן להיעזר בשירותיו של ספק חיצוני בשביל למלא תפקיד זה.

וכן, לפי ה-GDPR ובהתאם לסעי' שצוינו לעיל, לקבוצות וחברות יש שתי אפשרויות לעמוד בהתחייבותן למנות DPO. או שהם ממנים עובד כ-DPO, או שהם ממנים לכך אדם חיצוני. בבחירת אדם כזה, עליהם לוודא כי DPO פנימי אינו נתון לניגוד עניינים עקב עבודתו במחלקת ה-IT, במחלקת משאבי אנוש או בהנהלה הבכירה, שם יהיה עליו לפקח על עצמו. ללא קשר לאופציה שנבחרה, DPO חייב לספק ידע מקצועי ולהיות מומחה בדיני הגנת מידע ואבטחת מידע, ההיקף בהתאם למורכבות עיבוד הנתונים וגודל החברה.

DPO יוגדר על בסיס תכונות מקצועיות ובמיוחד ידע ומומחיות בדיני אבטחת מידע ושיטות עבודה ויכולת למלא את המשימות האמורות בסעיף 39.

משימותיו של ה-DPO:

- ליידע ולייעץ לבקר או למעבד ולעובדים המבצעים עיבוד על התחייבויותיהם בהתאם לתקנה זו ולהוראות אחרות של האיחוד או המדינות החברות בהגנה על מידע;
- לפקח על ציות לתקנה זו, להוראות אחרות להגנת מידע של האיחוד או המדינות החברות ולמדיניות של הבקר או המעבד ביחס להגנה על נתונים אישיים, לרבות הטלת אחריות, העלאת מודעות והכשרה של הצוות המעורב בעיבוד פעולות, והביקורות הנלוות;
- לספק ייעוץ כאשר מתבקש בכל הנוגע להערכת ההשפעה להגנה על נתונים ולפקח על ביצועיה בהתאם לסעיף 35;
- לשתף פעולה עם רשות הפיקוח;

- לשמש כנקודת המגע של רשות הפיקוח בנושאים הנוגעים לעיבוד, לרבות ההתייעצות המוקדמת האמורה בסעיף 36, ולהתייעץ, לפי הצורך, בכל עניין אחר.
- DPO יתחשב במילוי תפקידיו בסיכון הכרוך בפעולות העיבוד, תוך התחשבות באופיו, היקפו, ההקשר ובמטרות העיבוד.

לפי המלצות הרשות להגנת פרטיות בישראל:

ידע והכשרה: מומחיותו של ממונה ההגנה על הפרטיות נדרשת להיות משולבת, כך שתאפשר הבנה מיטבית של התהליכים בארגון ברמה הטכנולוגית והעסקית, לצד יכולת לבחון את התאמתם לדרישות החוק ולמדיניות הארגון.

כדי שיוכל למלא את תפקידו באופן אפקטיבי, תחומי הידע של ממונה הגנה על פרטיות צריכים לכלול לכל הפחות - ידיעה מעמיקה של דיני הפרטיות וההגנה על מידע אישי בישראל ובאירופה (לא בהכרח במסגרת השכלה משפטית פורמאלית)

הבנה מספקת בתחום טכנולוגיות המידע והבנה בסיסית בתחום אבטחת המידע, בשים לב להיקף ולמידה בהם הארגון מבוסס מידע וטכנולוגיה. דהיינו, ככל שליבת העיסוק של הארגון כרוכה בעיבוד מידע אישי, נדרשת מידת הבנה רבה יותר בתחום אבטחת המידע וטכנולוגיות המידע.

הכשרה ותחומי ידע נוספים העשויים לשפר את תפקוד ה-DPO ואת התועלת שתצמח ממנו לארגון: הכשרה אקדמית או מקבילה במשפטים, חשבונאות, טכנולוגיית מידע, ניהול תהליכים או ברגולציה;

היכרות עם דיני ההגנה על מידע אישי באירופה ובארצות הברית או בשווקים אחרים בעולם הרלוונטיים לארגון;

היכרות עם הפן העסקי של ניהול ארגון;

אתיקה.

לפי המלצות הרשות הצרפתית לאבטחת מידע ופרטיות (CNIL)

מי ניתן להגדרה כ-DPO:

למרות שאין פרופיל טיפוסי ל-DPO, ה-GDPR דורש מה-DPO שיהיה בעל רמת מומחיות.

על הארגון גם לוודא שאין ניגוד עניינים עם משימות אחרות של ה-DPO.

הידע והכישורים של ה-DPO:

• מומחיות משפטית וטכנית בנושא הגנת מידע;

• הכרת הקו העסקי, תקנות התעשייה וארגון המבנה עבור הארגון אליו הם מיועדים;

• הבנה של פעולות עיבוד, מערכות IT, הגנת הנתונים של הארגון וצרכי אבטחתו;

• לרשות ציבורית או לגוף ציבורי, היכרות טובה עם הכללים המנהליים והנהלים החלים.

התכונות האישיות הנחוצות לתפקיד ה-DPO:

ישרה גבוהה, רמת אתיקה מקצועית, יכולת לתקשר, יכולת שכנוע.

הערה: רמת המומחיות הנדרשת משתנה בהתאם לרגישות, המורכבות והנפח של נתונים המעובדים על ידי הארגון. ידע ומיומנויות אלו ניתן לרכוש באמצעות הכשרה ותוכנית מותאמת לפרופיל של ה-DPO העתידי.

האם DPO צריך להיות בעל תואר מסוים?

קבלת תואר מסוים או ביצוע הכשרה ספציפית אינה נדרשת כדי להיות מוגדר כ-DPO. יחד עם זאת, ה-DPO חייב להיות בעל כישורים וידע נאותים לביצוע תפקידיו.

לפיכך, אם ל DPO אין תואר המתמחה באבטחת מידע, ניתן להשלים את הכשרתו האקדמית עם ניסיון מקצועי או השכלה מתמשכת במחשבים, אבטחה, חוק ומשפט או כל נושא אחר הרלוונטי למילוי תפקידו.

לדוג', האם ניתן למנות עורך דין כ-DPO?

עורך דין יכול להיות מוגדר DPO של ארגון על בסיס חוזה שירות כ-DPO חיצוני. יחד עם זאת, עורך הדין לא יוכל לייצג ארגון זה בפני בתי המשפט במקרים הנוגעים לנושאים הקשורים לנתונים אישיים שכן ייצוג כזה יכול ויהיה בחזקת ניגוד עניינים.

תסקיר השפעה

תסקיר השפעה על פרטיות, המכונה לעיתים תסקיר השפעה על הגנת מידע, הוא תהליך אשר נועד לסייע לארגון באיתור, הערכה וניהול של סיכונים לפרטיות בפרויקטים או פעילויות עסקיות וארגוניות אחרות הכוללות עיבוד של מידע אישי.

https://www.gov.il/BlobFolder/reports/taskir_privacy/he/taskir_privacy.pdf



לאחר שבעל המאגר מצויד בתיק נהלי אבטחה כמתחייב בתקנות בהיותו בעל מאגר מידע עליו ליתן תוקף למספר תקנות כמתחייב בדין:

מס' תקנה	פירוט התקנה	מתן תוקף	הערות
2	מסמך הגדרות המאגר	אחת לשנה בכל שנה עד 31.12 לגבי שינויים טכנולוגיים/ארגונים משמעותיים ובהתקיים אירועי אבטחה	בשים לב לתקנה 2 (א)
4		אחת לשנה	האם יש צורך בעדכון הנוהל בשים לב לתקנה 4(ה)
5		ברמת אבטחה גבוהה סקר סיכונים ומבדקי חדירה – אחת ל- 18 חודשים	
7	אבטחת מידע בניהול כוח אדם	ברמת אבטחה בינונית או גבוהה הדרכת כ"א אחת לשנתיים	בשים לב לתכנים כאמור בתקנה 7 (ג)
9	זיהוי ואימות	ברמת אבטחה בינונית או גבוהה הדרכת כ"א אחת לשישה חודשים	בשים לב לתקנה 9 (ב) (2)
11	תיעוד של אירועי אבטחה	ברמת אבטחה בינונית דיון באירועי האבטחה ויבחן את הצורך בעדכוננו של נוהל האבטחה – אחת לשנה לפחות ברמת אבטחה גבוהה אחת לרבעון	
15	מיקור חוץ	חובתו של הגורם החיצוני לדווח, אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה אחת לשנה לפחות	בשים לב לתקנה 15 (ח)
16	ביקורת תקופתית	ברמת אבטחה בינונית או גבוהה ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה. אחת ל- 24 חודשים	בשים לב לתקנה 16 (א)

תיעוד של אירועי אבטחה-תקנה 11

https://www.nevo.co.il/law_html/law00/144811.htm

מיקור חוץ-תקנה 15

https://www.nevo.co.il/law_html/law00/144811.htm

הסכם למתן שרותי מיקור חוץ

שנערך ונחתם ב _____ ביום _____ בחודש _____ 2023

בין :

ח.פ.
(להלן: "בעל המאגר ו/או החברה")
-מצד אחד-

לבין :

ח.פ.
רח' , [מיקוד]
(להלן: "המחזיק ו/או מעבד המידע ו/או נותן השרות")
-מצד שני-

הואיל ובבעלות של _____ מאגר/ מספר מאגרי מידע (כפי וככל שיעודכן מעת לעת);

והואיל ו _____ מוגדרת כמחזיק ו/או כמעבד מידע (כהגדרתם בחוק הגנת הפרטיות, תשמ"א 1981-להלן: החוק) של מאגרי מידע של לקוחות רבים ומידע זה נשמר אצל _____ מתוקף היותו ספק צד ג' של _____, מתוקף זה הופכת _____ למחזיקה.

והואיל ו _____ מעניק/ה שירותי _____ (להלן "ההסכם"; "השירותים", בהתאמה);

והואיל ולצורך עמידה בדרישות דיני הפרטיות בכל הקשור לשימוש במאגר/י מידע, הצדדים מעוניינים להעלות על הכתב את הסכמותיהם בעניינים הללו, כפי שהן קיימות עובר למועד חתימת ההסכם, כמפורט בהסכם זה להלן;

לפיכך הוצהר, הוסכם והותנה בין הצדדים כדלקמן :

1. מבוא ונספחים

- 1.1. המבוא להסכם זה ונספחיו מהווים חלק בלתי נפרד ממנו ויפורשו ביחד עמו.
- 1.2. בכל מקרה של סתירה בין הוראות הסכם זה לבין נספחיו, תחול ההוראה המקיימת את דיני הפרטיות כהגדרתם להלן.

2. הגדרות

בהסכם זה תוקנה למונחים שלהלן המשמעות שלצידם, זולת אם משתמע אחרת מהקשר הדברים. למונחים שלא הוגדרו בהסכם זה תוקנה המשמעות שניתנה להם בחוק או בתקנות הרלבנטיות

- 2.1. "החוק" - חוק הגנת הפרטיות, תשמ"א-1981, כפי שיהיה בתוקף מעת לעת.
- 2.2. "תקנות אבטחת מידע" - תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, כפי שיהיו בתוקף מעת לעת.
- 2.3. "דיני הפרטיות" - החוק, תקנות אבטחת מידע, תקנות אחרות מכח החוק, הנחיות רשות הגנת הפרטיות, הנחיות והוראות ביצוע של כל רגולטור אחר החלות על _____, כבעלת מאגר מידע, הכל כפי שיהיו בתוקף מעת לעת.
- 2.4. "המידע" - "מידע" ו/או "מידע רגיש" כהגדרתם בחוק אשר נכללים במאגרי המידע של _____ או אשר יגיעו לידיעת _____ ו/או מי מטעמה באופן אחר והנוגעים ל_____ ו/או לשירותים, וכן כל מידע ש_____ תגדיר כמידע אישי, פרטי ו/או מידע המזהה או מאפשר זיהוי של אדם, אותם רשאי לעבד המחזיק בהתאם למטרות השימוש המוגדרות והמותרות בו בהתאם להסכם ולצורכי ההתקשרות בלבד.
- 2.5. "קבלן משנה" - כל ספק או קבלן משנה המועסק על ידי _____ בקשר עם השירותים ו/או ההסכם, אשר תהיה לו באופן כלשהו גישה למידע, ובכלל זה ספקי שירותי ענן ו/או גורם חיצוני המספק לספק שירותי אחסון ו/או גיבוי למידע.
- 2.6. "שימוש במידע" - כל פעולה במידע, לרבות איסוף, תיעוד, ארגון, גישה, עיבוד, אחסון, אירוח, שמירה, תחזוקה, שירות, התאמה, שינוי, טיוב, גילוי, העברה, מסירה, השמדה או מחיקה.
- 2.7. "אירוע אבטחת מידע" - כל אירוע של תקיפת מערכות מידע או אמצעי טכנולוגי אחר ששייכים ל_____ ו/או לקבלן משנה, העלולה לפגוע בסודיות, שלמות או זמינות מערכות או מידע של _____, לרבות אירוע בו נעשה שימוש במידע בלא הרשאה או בחריגה מהרשאה.
- 2.8. "מערכות" - תשתיות, מערכות האחסון והשרתים המכילות את המידע.
- 2.9. "מאגר מידע", "מחזיק" או "מחזיק במאגר מידע" - כהגדרת מונחים אלה בחוק.

3. מידע, מערכות המאגר והעיבוד המותג

- 3.1. המחזיק יהא רשאי ו/או יוכל לעשות שימוש ו/או עיבוד במידע של בעל המאגר עליו יוסכם בין הצדדים ויפורט בהסכם זה, בהתאם להגדרת תפקידו של המחזיק ולשירותים אותם יספק לבעל המאגר, בכפוף למטרות השימוש המותרות בו לצורכי ההתקשרות בהסכם זה.
- 3.2. מערכות המאגר ו/או המידע בהן יוכל המחזיק לעשות שימוש ו/או עיבוד בהתאם להסכם, הינן כדלקמן: א. _____
ב. _____
ג. _____
- 3.3. המחזיק יהא רשאי לבצע עיבוד _____ ו/או לבצע _____ על המידע המפורט לעיל.
- 3.4. משך ההתקשרות בין הצדדים הינו מיום חתימת הסכם זה או החל מיום _____ ועד ליום _____ /לתקופה בת _____ החל מיום _____, כמוסכם בין הצדדים (להלן-"תקופת ההסכם").

4. הצהרות והתחייבויות

מצהירה ומתחייבת כי:

- 4.1 תמלא אחר כל המוטל עליה כ"מחזיק" ו/או כ"מעבד מידע", ותשמור את המערכות המכילות את מאגרי המידע של _____
- 4.2 ידוע לה שהבעלות במאגרי המידע ובמידע המצוי בהם הינה של _____ וכי מוטלות על _____ חובות כלפי נשואי המידע. _____ לא תעשה שימוש במידע אלא לצורך ביצוע השירותים לפי הסכם זה ו/או כל הסכם בכצב שיבוא בנוסף ו/או במקומו אלא אם _____ אישרה אחרת בכתב.
- 4.3 העונה על כל דרישות החוק ותקנות אבטחת המידע. במועד חתימת נספח זה, ממונה אבטחת המידע מטעם _____ הינו/ה _____ ("הממונה"), אשר ישמש כאיש הקשר בין _____ לבין _____ בכל הקשור ליישומו של נספח זה. _____ תעדכן את _____ בדבר שינוי בזהות הממונה.
- 4.4 ידוע לה שכל מידע שיועבר ו/או יגיע אליה במסגרת או לצורך ביצוע השירותים ייחשב כ"מידע סודי" של _____, _____ תשמור עליו בסודיות בהתאם לתנאי הסודיות המקובלים בין שתי החברות.
- 4.5 תודיע ל _____ על כל פניה מצד נושא מידע בקשר עם זכויות העיון המוקנות לו עפ"י דיני הפרטיות, ותסייע ל _____ בטיפול בפניות אלה ככל שתידרש.
- 4.6 בתום תקופת ההסכם כמפורט בסעי' 3.4 לעיל, ישיב המחזיק את המידע לבעל המאגר ו/או ישמיד את המידע מרשותו ו/או מרשות כל מי מטעמו ו/או כל קבלן משנה. בסיום השבת המידע לבעל המאגר והשמדתו כאמור, ידווח המחזיק על כך לבעל המאגר.

5. גישת עובדי _____ למידע

מצהירה ומתחייבת כי:

- 5.1 אין לה ו/או למי מטעמה גישה למידע עצמו, אלא לתשתיות ולמערכות האחסון והשרתים המכילות את המידע.
- 5.2 הגישה למערכות תתאפשר לעובדי _____ שלא הורשעו בעבירות בקשר לשימוש במידע, שגישתם למידע נדרשת לצורך ביצוע השירותים בלבד, על בסיס הצורך לדעת ובמתכונת המצומצמת ביותר האפשרית. _____ תבחן את הרשאות הגישה באופן רבעוני ותבטל הרשאות עודפות.
- 5.3 וטרם ביצוע השירותים על גישת עובדי _____ למידע תהא מאובטחת (ברמה הפיזית והלוגית), ידם - יחתמו על התחייבות כלפי _____ לסודיות ואבטחת מידע, בנוסח המקובל ב _____ . העתקי התחייבויות הנ"ל יועברו ל _____ עפ"י דרישתה.
- 5.4 תדריך כל עובד כאמור טרם תחילת ביצוע השירותים על ידו, באשר למטרות השימוש במידע, וחובותיו לסודיות ואבטחת מידע בהיקף הנדרש לביצוע תפקידו. הדרכות נוספות יבוצעו על בסיס שנתי לפחות לעובדים קיימים, ולכל עובד חדש טרם תחילת ביצוע השירותים על ידו. _____ תתעד ביצוע ההדרכות (לרבות היקפן והעובדים שעברו אותן) ותעביר ל _____ דו"ח בנושא מידי שנה.
- 5.5 תישא באחריות כוללת למעשי ו/או מחדלי עובדיה בקשר עם נספח זה.

6. קבלני משנה

- 6.1 מצהירה שידוע לה כי העסקת קבלני משנה תהא מותנית: (א) באישור מראש ובכתב של _____; (ב) בבדיקת

_____ כי לא קיים חשש לניגוד עניינים או סיכון אחר לשימוש פסול במידע ע"י קבלן המשנה; (ג) ובהחתמת קבלן המשנה על הסכם (כאמור בסעיף 5.2. רשימת קבלני משנה, סוג השירות שניתן ע"י כל אחד ומאגרי המידע אליהם יש לקבלן המשנה גישה לשם כך תועבר ל _____ עפ"י דרישתה.

6.2. כל ספק משנה מאושר שעומו תתקשר _____ יהיה חייב, כתנאי מוקדם להיותו ספק משנה בקשר עם השירותים, להתחייב כלפי _____ בהתחייבויות מקבילות להתחייבויות _____ כלפי _____ על פי הסכם זה באופן שספק המשנה יתחייב (בין בעצמו, ובין ביחס לכל מורשי גישה מטעמו) ביחס למידע של _____ לקיים, לכל הפחות, אותה רמת הגנה ואבטחת מידע החלה על _____ על פי נספח זה. העתק ההסכמים בין _____ לבין ספקי המשנה ימסר למזמין, על פי דרישה.

6.3. _____ תפקח ותבקר אחר פעילות קבלני המשנה, ותסיים לאלתר כל התקשרות עם קבלן משנה שאינה עומדת בדרישות נספח זה. _____ תישא באחריות כוללת למעשי ו/או מחדלי קבלני המשנה שיועסקו על ידה.

מחיקת מידע

.7

7.1. במהלך ביצוע השירותים בתקופת ההסכם, ובכל מקרה של סיום או הפסקת ההתקשרות בין הצדדים מכל סיבה שהיא, _____ תהיה רשאית לדרוש מ _____ להעביר ל _____ מידע ממאגרי המידע, או למחוק מידע כאמור (כולו או חלקו, לפי העניין) באופן שאינו ניתן לאחזור או שחזור, והכל – בין אם מידע כאמור מצוי ברשות _____ ו/או ברשות קבלני משנה מטעמה. _____ מתחייבת לפעול על פי דרישתה של _____, לתעד את פעולות העברת ו/או השמדת ומחיקת המידע, ולספק ל _____ תצהיר בדבר עמידתו בדרישות אלה.

7.2. ככל שקיימת הוראה בדין המחייבת שמירת המידע לאחר תום תקופת ההתקשרות – _____ תשמור את המידע המינימאלי הנדרש, ותיישם את כל אמצעי אבטחת המידע הדרושים ביחס לאותו מידע.

אבטחת מידע

.8

8.1. _____ תפעל על פי הוראות דיני הפרטיות בכל הקשור והנוגע לאבטחת המידע במאגרי המידע של _____ (בהתאם לרמות האבטחה שסווגו להם), וכן עפ"י נהלי והנחיות _____

8.2. מבלי לגרוע מהאמור, _____ מתחייבת: (א) לא לבצע שינויי הגדרות של אמצעי אבטחת מידע ללא אישור _____ מראש; (ב) ליצור הפרדה (פיזית ולוגית) בין הפעילות שתבצע עבור _____ במסגרת השירותים לבין פעילויות אחרות המבוצעות על ידה (עבור עצמה או ללקוחות אחרים); (ג) להכין מסמך מיפוי של מערכות המידע ב _____ בהן אגור המידע, לעדכן אותו ככל שנדרש ולחשוף אותו בפני מורשי הגישה הרלבנטיים בלבד; (ד) להכין נהלי אבטחת מידע התואמים את רמת/ות אבטחת המידע ביחס למאגרי המידע שבחזקתה, בהתאם לתקנות אבטחת המידע, ולעדכן אותם במידת הצורך; (ה) לקיים מנגנון אוטומטי של תיעוד ובקרת גישה (פיזית ולוגית) למאגרי המידע של _____ בהתאם לדרישות תקנות אבטחת המידע.

אירועי אבטחת מידע

.9

9.1. _____ תודיע ל _____ מיד, ולא יאוחר מ- 12 שעות מהמועד בו נודע לה, או לקבלן משנה מטעמה, על כל אירוע אבטחת מידע בקשר עם המידע או מאגרי המידע של _____ . _____ תמשיך לדווח ל _____ באופן שוטף על כל מידע נוסף שיובא לידיעתה או לידיעת קבלני המשנה שלה, בקשר עם אירוע אבטחת המידע.

9.2. _____ תשתף פעולה עם _____ בכל הנוגע לחקירת אירוע אבטחת מידע, הערכת מצב, הכלה ובלימה והצעדים שיש לנקוט בעקבותיו, התאוששות חזרה לשגרה, וכן מתחייבת לא לדווח על אירוע כאמור לכל גורם חיצוני (למעט אם עפ"י יעוץ משפטי שקיבלה – חלה עליה חובת דיווח כאמור, ובמצב זה תמסור על כך הודעה לאלתר ל _____, ותפעל בתיאום ושיתוף פעולה עימה).

9.3. בנוסף, _____ תעניק גישה מלאה ל _____ ולכל מי מטעמה לנתונים פורנזיים ככל ואלה יידרשו לצורך חקירת אירוע אבטחת המידע. לחילופין תשתף _____ את _____ ו/או מי מטעמה בדו"ח הממצאים של אירוע אבטחת המידע.

10. דיווח, ביקורת ובקרה

10.1. _____ תדווח ל _____ באופן שנתי לפחות בדבר אופן עמידתה בחובותיה כמחזיק על פי דיני הפרטיות בקשר עם ביצוע השירותים.

10.2. _____ תאפשר ל _____ ו/או לרשויות שונות לבצע ביקורות באתריה, תשתף פעולה עם ביקורות כאמור ותעביר לגורמים המבקשים את החומרים הרלבנטיים לביקורת. ביקורות מצד _____ יבוצעו לצורך בדיקת עמידת _____ בהתחייבויותיה מכח נספח זה, בשעות העבודה המקובלות, ובליווי נציג מטעם _____ תהא אחראית לאכוף דרישות אלה על קבלני המשנה מטעמה.

11. שונות

11.1. כל שינוי בהסכם זה (לרבות שינוי שיבוצע ע"י _____ לצורך עמידה בדיני הפרטיות – לרבות כתוצאה משינוי חקיקה, הנחיה רגולטורית, אירוע אבטחת מידע וכו') יערך בכתב וייחתם על ידי שני הצדדים. _____ תהא אחראית ליישם כל שינוי כאמור גם אצל קבלני המשנה שלה.

11.2. הצדדים מתחייבים להודיע, בכתב, כל צד למשנהו, אודות כל תביעה אשר תוגש על ידי צד שלישי כנגד מי מהצדדים בקשר עם הסכם זה וכן אודות כל דרישה אשר תתקבל על ידם מהרשויות בכל הקשור להסכם זה.

11.3. ככל שיידרש, _____ תחתום על כל מסמך רלבנטי ותנקוט בכל פעולה הנחוצה לצורך הוצאתו לפועל של הסכם זה ולצורך עמידת הצדדים בדרישות דיני הפרטיות החלות עליהם.

11.4. _____ אינה רשאית להעביר ו/או להסב ו/או להמחות את התחייבויותיה על פי הסכם זה לצד שלישי כלשהו מבלי לקבל על כך את הסכמת מראש ובכתב.

11.5. הנני מצהיר/ה כי קראתי את תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 בדגש על תקנות 15 ו- 19 והנני מתחייב/ת לפעול על פי הן.

ולראיה באו הצדדים על החתום :

המחזיק ו/או מעבד המידע
ו/או נותן השרות"

בעל המאגר ו/או החברה