

מדריך פעולה ליישום תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) בעת

התקשרות עם גורם חיצוני¹

1. כללי:

בשנים האחרונות, גוברת מגמת ההסתייעות של ארגונים רבים, הן במגזר הפרטי והן במגזר הציבורי, בנותני שירותים חיצוניים דרך מיקור חוץ, שניתנת להם גישה גם למאגרי המידע האישי של הארגון (להלן גם: "הספק" או "גורם חיצוני"). לשימוש בספקים יתרונו רבים, כאשר הצורך העיקרי בהם נובע מהרצון להתייעלות מקצועית וכלכלית בארגון.

ככלל, ספקים מתאפיינים בכך שאינם חלק מהמערך הארגוני ואינם נמנים על עובדי הארגון. כמו כן, במקרים רבים, ספקים נותנים שירות למגוון ארגונים במקביל. שני מאפיינים מרכזיים אלו, טומנים בחובם שורה של סיכונים סייבר ואבטחת מידע. **בהיבטי אבטחת מידע מרבית הסיכונים טמונים בסוגיות של גישת הספק למידע האישי בארגון, העברת מידע בין הספק לארגון וסיום ההתקשרות ביניהם.**

מאחר שישנן משמעויות משפטיות, עסקיות וטכנולוגיות לשימוש במיקור חוץ הכולל מתן גישה למידע האישי המוחזק בארגון, מטרת תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "התקנות"), היא להסדיר את אופן ההתקשרות בין הארגון לבין כל גורם חיצוני (שאינו אדם יחיד), המספק לארגון שירות הכרוך במתן גישה למאגר המידע שלו.

מטרת מדריך פעולה זה היא להנחות את הארגונים בדבר הפעולות שעליהם לבצע לצורך עמידה בתקנה 15 לתקנות.

לפי תקנה זו, על בעל מאגר מידע חלות חובות שונות כתנאי להתקשרות עם ספק חיצוני:

א. חובה לערוך בדיקה האם הסיכונים הכרוכים בהתקשרות עם הספק מאפשרים את ההתקשרות עמו. ככלי עזר לביצוע הבדיקה, רשאי בעל המאגר להסתייע בשאלון הבדיקה המוצע בנספח א' (להלן - **שאלון הבדיקה המקדמי**), תוך התאמתו לנסיבות הספציפיות של השירות ושל המידע המעובד, ובחינתו אל מול רגישות המידע המעובד והסיכונים הספציפיים הנובעים מן ההתקשרות.

ב. חובה לקבוע הוראות מפורטות בנוהל אבטחת המידע בנושאים המפורטים בתקנה 15, וכן החובה לנקוט אמצעי פיקוח ובקרה על הספק – בהיקף ההולם את הסיכונים הספציפיים הנובעים מההתקשרות עמו. ככלי עזר ודוגמה לאמצעי פיקוח ובקרה, יכול בעל המאגר להסתייע בנספח ב', שמטרתו לסייע לבעל המאגר לוודא את עמידת הספק בהוראות החוק

¹ מדריך זה מתפרסם ככלי עזר לבעלי מאגרי מידע. האמור בו אינו ממצה את דרישות תקנה 15 ואת חובות בעל המאגר, ואינו פוטר את בעלי המאגרים מקיום כל הוראות חוק הגנת הפרטיות והתקנות שנקבעו מכוחו, בשם לב לנסיבות הספציפיות של כל מאגר מידע וכל שירות.

והתקנות, ובהסכם מיקור החוץ. זאת, באמצעות קבלת מענה של הספק לשאלון הנ"ל (להלן – **שאלון הבקרה התקופתית**), תוך התאמתו לנסיבות הספציפיות של השירות, סוג המידע הנוגעים בדבר ונקיטת אמצעי פיקוח ובקרה נוספים ככל הנדרש בעייתיים.

ג. חובה לערוך הסכם כתוב ומחייב מבחינה משפטית בין בעל המאגר לבין הספק, על מנת לקבוע בו הנחיות מפורשות, בהתאם לסוג השירות אותו הוא מבקש לקבל. לשם כך, יש לאפיין את מהות השירות, את תהליכיו העסקיים והטכנולוגיים (מערכות המידע ונכסי המידע הרלוונטיים להתקשרות), את מורשי הגישה של הספק למערכות הרלוונטיות ואת האופן בו ייגשו למידע, ולבסוף את הסדרת סיום או שינוי ההתקשרות.

2. פירוט תוכן ההסכם המתחייב עם הספק לפי תקנה 15(א)(2):

הערות	ביצוע	סעיפי תקנה 15(א)(2):
	יש לנסח סעיף שיגדיר במפורש את סוג המידע שאליו רשאי הספק לגשת, ואת מטרת השימוש לכל סוג של מידע..	(א) המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות;
ניתן להסתייע במסמך מיפוי מערכות המאגר ולוודא כי הינו מעודכן.	ככל שהספק נדרש לקבל הרשאות גישה למערכות המחשוב של בעל המאגר, יש לפרט אודות מערכות אלו ואודות מורשי הגישה מטעם הספק שמקבלים הרשאת גישה.	(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;
	בהמשך ישיר לסעיף הקודם, יש לפרט באופן רחב יותר מה הספק רשאי "לעשות" עם המידע. למשל, האם מדובר בצפייה בנתונים בלבד, או שמא הספק רשאי גם לכתוב מידע חדש או לשנות את הקיים.	(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;



הערות	ביצוע	סעיפי תקנה 15(א)(2):
	יש לציין את תוקף ההסכם, כלומר, את מועד סיום ההתקשרות בין הספק לבעל המאגר. כמו כן יש לתאר את האופן בו הספק ישיב או ישמיד את המידע שקיבל מבעל המאגר, בסיום ההתקשרות. למשל, אם מדובר בקבצים – יש למחקם מכל מערכת בה עובדו, לרבות תיבות דוא"ל, תיקיות ואף גיבויים. דוגמה נוספת היא שאם מידע הועבר דרך התקן חיצוני כלשהו או מחשב נייד, יש להשיבם לבעל המאגר. יש לוודא בסיום ההתקשרות כי הספק מעביר לבעל המאגר דיווח הכולל אישור סופי ומחייב על ביצוע ביעור/מחיקה/השמדה/השבה של כל מידע רלוונטי כאמור.	(ד) משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;



הערות	ביצוע	סעיפי תקנה 15(א)(2):
מומלץ טרם ההתקשרות עם ספק, לבדוק תחילה האם חיוני להעביר אליו מידע אישי, או שניתן להסתפק במתן גישה מוגבלת בזמן לתקופת מתן השירות דרך מערכות המידע של בעל המאגר. טרם ההתקשרות יש לבחון את סיכוני אבטחת המידע הכרוכים בהתקשרות; מומלץ לעשות זאת באמצעות סקר סיכונים כמשמעותו בתקנה 5(ג).	ככל שהספק הוא גם "מחזיק" (קרי, מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש, אך הוא אינו בעל המאגר), על ההסכם לפרט את אופן עמידתו בכלל חובותיו לפי התקנות, לרבות מתן הנחיות פרטניות ליישומן. ² יודגש כי החוק והתקנות מטילים על "מחזיק" אחריות ישירה לאבטחת המידע במאגר לגביו הוא נותן שירות, גם מעבר לאחריותו החוזית מול בעל המאגר. כמו כן, מוטלת על המחזיק, לצד בעל המאגר, חובת הדיווח המיידית לרשות להגנת הפרטיות על קרות אירוע אבטחה חמור.	(ה) אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;
	יש לציין בפני הספק, כי עליו לחתום על הסכמים מול עובדיו (מכל סוג העסקה), בהם יעגן את חובותיהם לסודיות ועמידה בהסכם שנקבע בין בעל המאגר לבין הספק.	(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);

² לעניין היחס בין "מחזיק" לפי חוק הגנת הפרטיות לבין "גורם חיצוני" לפי תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), ראו הבהרה שפרסמה הרשות להגנת הפרטיות במסגרת שאלות ותשובות בעניין זה: https://www.gov.il/he/departments/guides/data_security_fqa:chapterIndex=5



הערות	ביצוע	סעיפי תקנה 15(א)(2):
מדובר במקרה שבו הספק מתכוון לעשות שימוש בשירות מיקור חוץ מטעמו (כגון קבלן/ספק משנה). במקרים שכאלה מדובר בהחמרה של רף הסיכונים לאבטחת המידע של בעל המאגר, ולכן יש לקחת סיכונים אלו בחשבון טרם ההתקשרות עם ספק כאמור.	אם הספק נותן שירות באמצעות ספק משנה נוסף, עליו לקבוע הסכם עם אותו ספק משנה, ולוודא כי גם הסכם זה כולל את כל העניינים המפורטים כאן.	ז) התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו;
ככל שמשך ההתקשרות ארוכה יותר, כך עולה הסיכוי לשינויים שונים ומגוונים אצל הצדדים להסכם, ולכן הביקורת על אופן העמידה בהוראות תקנה 15(א) עולה בחשיבותה. יש לוודא כי הגורם החיצוני מתעד ומנהל כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלימות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה.	יש לקבוע סעיף המגדיר במפורש את הנוהל בו מדווח הספק לבעל המאגר על אופן ביצוע חובותיו ועמידתו בכלל הוראות הסכם זה.	ח) חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה;

3. יובהר, כי מלבד ההוראות האמורות בעניין תוכן ההסכם בין בעל המאגר לבין הגורם החיצוני, תקנה 15 מחייבת את בעל המאגר לבחון, לפני ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בה (תקנה 15(א)(1)); לפרט בנוהל אבטחת המידע של המאגר את הנושאים הקבועים בתקנות 15(א)(2)-(ה), תוך הפניה מפורשת להסכם עם הגורם החיצוני ולנוהל האבטחה שלו (תקנה 15(א)(3)); ולנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם

ובתקנות אבטחת מידע, בהיקף הנדרש בשים לב לסיכוני אבטחת המידע הקיימים ביחס לאותו גורם חיצוני (תקנה 15(א)(4)).

4. באתר הרשות להגנת הפרטיות, ניתן למצוא פרסומים נוספים הכוללים הסברים ודוגמאות לדרישות החוק והתקנות ביחס למיקור חוץ הכרוך בגישה למידע אישי:

- 4.1.1 הנחיית רשם מאגרי מידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי"³
- 4.1.2 עמוד מידע בנושא אבטחת מידע בהתקשרות עם ספקים חיצוניים באתר הרשות.⁴
- 4.1.3 עמוד שאלות ותשובות באתר הרשות בנושא מיקור חוץ.⁵
- 4.1.4 פרק בנושא מיקור חוץ מתוך "המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע)".⁶

5. הרשות מוצאת לנכון להבהיר, כי הנספחים להלן משמשים ככלי עזר בלבד, ואין להשתמש בהם בלבד כדי למלא את הוראות החוק והתקנות. על כל בעל מאגר לוודא, בהתאם לתקנות עצמן, כי הוא ממלא אחר כל היבטי אבטחת המידע אל מול ספק מיקור החוץ.

³ הנחיית רשם מאגרי מידע מס' 2/2011 זמינה בקישור:

<https://www.gov.il/he/departments/policies/outsourcing>

⁴ עמוד המידע בנושא אבטחת מידע בהתקשרות עם ספקים חיצוניים זמין בקישור:

https://www.gov.il/he/Departments/General/data_security_outsourcing

⁵ עמוד שאלות ותשובות באתר הרשות בנושא מיקור חוץ:

https://www.gov.il/he/departments/guides/data_security_fqa?chapterIndex=5

⁶ הפרק בנושא מיקור חוץ, בתוך המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע), הזמין בקישור:

https://www.gov.il/he/Departments/Guides/data_security_guide?chapterIndex=17



נספח א'

שאלון בדיקה - היבטי אבטחת המידע של הספק

מס'	השאלה
1.	האם לספק החיצוני יש קובץ נהלי אבטחת מידע מעודכן ?
2.	האם הספק מחזיק בתו תקן תקף בנושא אבטחת מידע בנוסף לעמידתו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017?
3.	האם הספק מחזיק בתיעוד מסודר של מערך השרתים והאפליקציות בשימוש הלקוחות?
4.	האם ברשת של הספק קיימת חלוקה לפי ייעוד סיגמנטציה ?
5.	האם הספק מקיים הדרכות לעובדיו בתחום אבטחת מידע והעלאת מודעות לאופן השימוש במאגרי מידע?
6.	האם הספק שומר לוגים או מנגנוני תיעוד אחרים עבור כל הפלטפורמות שיש ברשותו, כולל מערכות ההגנה והאפליקציות?
7.	האם נתוני התיעוד של מנגנון הבקרה והלוגים נשמרים לפרק זמן של לפחות 24 חודשים?
8.	האם לספק החיצוני יש נוהל טיפול באירועי סייבר? והאם קיים נוהל או תכנית עבודה להתאוששות מאירוע סייבר?
9.	האם הספק שומר עותק גיבוי למידע של הלקוחות שלו? במידה וכן, האם יש נוהל מסודר לאופן ביצוע הגיבויים, ובפרט האם המידע המגובה נשמר באופן מוצפן?
10.	האם מערכות ההפעלה של תחנות הקצה ומערכות ההפעלה של הספק מאובטחות כראוי על ידי מערכת EDR?
11.	האם הספק משתמש באמצעי אבטחה (זיהוי דו שלבי) לצורך מתן גישה מרחוק למאגרי המידע של לקוחותיו?
12.	האם הספק עושה שימוש במערכות ההגנה (כגון WAF)?
13.	האם הספק מבצע בדיקות על ידי גורם חיצוני בלתי תלוי בנושא ניהול סיכונים אבטחת המידע?
14.	האם התקיים אצל הספק בשלוש השנים האחרונות אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (אירוע אבטחה כמשמעותו בסעיף 11(א) לתקנות האבטחה) או אירוע סייבר שפגע בתפקוד או בהמשכיות הפעילות העסקית שלו? אם כן נא לפרט
	האם התקיים אצל הספק בשלוש שנים האחרונות אירוע אבטחה חמור המחייב דיווח לרשות להגנת הפרטיות? אם כן נא לפרט
15.	האם הספק מנהל יומן תיעוד מסודר לאירועי האבטחה? אם כן



השאלה	מס'
האם התנהל נגד הספק הליך פיקוח או אכיפה של הרשות להגנת הפרטיות ב-5 השנים האחרונות? אם כן נא לפרט את טיבם ותוצאותיהם	16.
האם הוגשו נגד הספק תביעות אזרחיות בנושא פרטיות או אבטחת מידע? אם כן נא לפרט	17.



נספח ב'

שאלון בקרה תקופתית

מדי שנה ממועד ביצוע ההתקשרות, מומלץ להעביר לספק החיצוני את השאלון שלהלן, וכן לדרוש ממנו דיווחים מידיים לכל הפחות בנסיבות המפורטות להלן:

מס'	שאלה
1.	האם בוצעו שינויים משמעותיים בתשתיות המחשוב? במידה וכן, האם בוצעה בדיקה על ידי גורם חיצוני בלתי תלוי לבחינת תקינת תשתיות המחשוב?
2.	האם בוצעה לעובדים הדרכה בתחום אבטחת מידע והעלאת מודעות בנוגע לאופן השימוש במאגרי מידע?
3.	האם הספק ביצע בדיקות לצורך תיקוף או הארכת תוקף תו התקן שיש ברשותו, ככל שיש ברשותו תו תקן תקף?
4.	האם הספק חווה אירוע אבטחת מידע או אירוע סייבר?
5.	דיווח מידי לבעל המאגר על כל פתיחה של הליך פיקוח או פניה מצד הרשות להגנת הפרטיות או של רגולטור אחר בנושאים הקשורים לפרטיות, אבטחת מידע או הגנת סייבר.
6.	דיווח מידי לבעל המאגר על קבלת מכתבי תלונה, התראה לפני תביעה, או הגשת תביעה אזרחית בנושאים של פרטיות או אבטחת מידע.
7.	האם הספק החתים את כל בעלי ההרשאות שלו להתחייבות לשמור על סודיות המידע, ועמידה בהסכם שנקבע בינו לבין בעל המאגר.
8.	ככל שהספק נדרש לשירותי גורם נוסף לצורך מתן השירות לבעל המאגר, האם נכלל בהסכם הספק לבין הגורם הנוסף כל הנושאים המפורטים בהסכם שיש בינו לבין בעל המאגר?