מעו"דכן טכנולוגיות מידע ופרטיות **ספטמבר 2023**

<u>מדריך ליישום תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) בעת התקשרות עם גורמים חיצוניים</u>

לקוחות יקרים,

בעדכון זה נציג בפניכם את המדריך שפרסמה הרשות להגנת הפרטיות בכל הנוגע להתקשרויות עם גורמים חיצוניים במיקור חוץ (Outsourcing). מטרת המדריך היא לספק לארגונים הנחיות בכל הנוגע לפעולות שעליהם לבצע לצורך עמידה בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("**התקנות**") בעת התקשרותם עם ספקים חיצוניים.

היות שספקים חיצוניים אינם חלק מהארגון ואינם נחשבים לעובדי הארגון, ומאחר שבמקרים רבים, ספקים אלו נותנים שירות למגוון רחב של ארגונים במקביל; מתעוררים מספר סיכוני סייבר ואבטחת מידע אליהם התייחסה הרשות להגנת הפרטיות ("**הרשות**"). הסיכונים העיקריים לדעת הרשות נמצאים בכל אחד מהמצבים הבאים:

א. מתן גישה לספק למידע האישי בארגון;

ב. העברת מידע בין הספק לארגון;

ג. בעת סיום ההתקשרות.

<u>המדריך מבהיר את החובות החלות על בעלי מאגרי מידע כתנאי להתקשרות עם ספקים חיצוניים</u>:

- **לפני ההתקשרות - חלה חובה לבדוק האם הסיכונים הכרוכים בהתקשרות עם הספק מאפשרים את ההתקשרות איתו**. לצורך כך, הרשות פרסמה שאלון בדיקה מקדמי (המצורף מטה), בו ניתן להיעזר כדי לבצע את הבדיקה.
- **חובה לקבוע הוראות מפורטות בנהלי אבטחת המידע בנושאים המפורטים בתקנה 15, וכן חובה לנקוט באמצעי פיקוח ובקרה ההולמים את הסיכונים הספציפיים שנובעים מההתקשרות עם הספק**. לשם כך, הרשות פרסמה שאלון בקרה תקופתית (המצורף מטה) על מנת לסייע לבעל המאגר המידע לוודא האם הספק עומד בדרישות החוק, התקנות ובהסכם מיקור החוץ.
- **חובה לערוך הסכם מחייב בכתב בין בעל המאגר לבין הספק, שיציין הנחיות מפורשות בהתאם לסוג השירות שבעל המאגר מבקש לקבל**.[1] לשם כך, יש לפרט על מהות השירות, תהליכיו העסקיים והטכנולוגיים, מורשי הגישה של הספק ואת האופן בו ייגשו למידע, ולבסוף את הסדרת סיום או שינוי ההתקשרות.

מחלקת סייבר וטכנולוגיות מידע במשרדנו מלווה לאורך השנים שורה ארוכה של ארגונים בניהול התקשרויות עם צדדים שלישיים בהם מועבר מידע אישי ובתהליכי ציות וביקורת לעמידה בהוראות התקנות. נשמח לעמוד לרשותכם בכל שאלה בעניין זה.

---

[1] המדריך מנחה ומפרט כיצד יש לבצע את הוראות ההסכם שיקבע בין בעל מאגר המידע לספק בהתאם לסעיפי תקנה 15(א)(2).

אנו עומדים לרשותכם בכל שאלה או הבהרה ונשמח לסייע ככל הנדרש.

למידע נוסף ניתן לפנות אל:

עו"ד עמית דת	**adat@fbclawyers.com**	**03-6941320**
עו"ד עמרי רחום-טוויג	**orachum@fbclawyers.com**	**03-6941320**
עו"ד ג'ודי עמידור	**jamidor@fbclawyers.com**	**03-6091116**
עו"ד לני צבעוני	**lzivoni@fbclawyers.com**	**03-6091116**

.....

הכלול באגרת מידע זו הוא מידע כללי בלבד, הוא אינו חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו. כל הזכויות שמורות לפישר ושות'. להרשמה למייל זה או להסרה מרשימת התפוצה - newsletter@fbclawyers.com

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

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?