אם אינך רואה מייל זה לחץ כאן

כניסתם לתוקף של חוקים חדשים באיחוד האירופי הנוגעים לאבטחת סייבר

24 בנובמבר, 2024

בשנים האחרונות נעשים מאמצים רבים במדינות שונות ברחבי העולם לקבוע חוקים ותקנות הנוגעים לאבטחת מידע, הן בהיבטי פרטיות ושמירה על מידע אישי והן בהיבטי הגנת סייבר ואבטחה באופן רחב. בחודש דצמבר 2022 אימץ האיחוד האירופי את תקנות NIS 2, שמטרתן לקבוע סטנדרט אבטחת מידע מינימלי לחברות וגופים בתחומים ממוקדים אשר מוגדרים כ-"חיוניים" (Essential) או "חשובים" (Important), כגון חברות וגופים בתחומי האנרגיה, הבנקאות והשווקים הפיננסיים, הבריאות, התשתיות הדיגיטליות ועוד. עם אימוץ התקנות, נקבע כי עד ליום 17 באוקטובר, 2024, יהיה על המדינות החברות באיחוד האירופי לקבוע חוקים מדיניים המאמצים את דרישות NIS 2, ומחילים אותן ברמה המדינתית החל מה-18 באוקטובר 2024. בנוסף, אנו מתקרבים לתאריך היעד של תחילת התחולה של ה-Digital Operational Resilience Act (DORA), הנוגעת לדרישות אבטחת מידע במגזר הפיננסי האירופי בפרט, אשר נקבע ל-17 בינואר 2025.

חברות ישראליות עשויות לפגוש את תקנות NIS 2 ואת תקנות DORA בכמה אופנים:

1. כאשר יש להן חברות בנות או חברות אם אשר הוקמו באירופה;
2. כאשר הן עצמן מספקות שירותים שונים באירופה;
3. בצורה עקיפה דרך דרישות חוזיות מלקוחות אירופאיים אשר ידרשו עמידה בתקנות כחלק מההתקשרות.

בהתאם לכך, ראינו לנכון לרענן את הדרישות הבסיסיות שמחילות תקנות NIS 2 ו-DORA, כדי שקהל לקוחותינו יוכל לוודא שהוא עומד בהן כנדרש.

מי כפוף לדרישות של תקנות NIS 2?

כאמור, תקנות ה-NIS 2 חלות על שני סוגי גופים – חברות "חיוניות" (Essential) וחברות "חשובות" (Important). חברות חיוניות מוגדרות כאחד מסוגי החברות הבאים:

1. חברות בתחומים המנויים בנספח הראשון לחוק, ואשר מעסיקות מעל 250 עובדים ושמחזור העסקים השנתי שלהן גבוה מ-50 מיליון אירו. נזכיר כי התחומים המפורטים בנספח הראשון כוללים חברות מתחומי האנרגיה, התחבורה, הבנקאות והשירותים הפיננסיים, הבריאות, מי שתייה, טיפול וניהול מי שופכין, תשתיות דיגיטליות (כגון ספקי שירותי DNS, ספקים של שירותים חישוב בענן, ועוד), ספקים של שירותי אינטרנט ותקשוב (כגון שירותי MSSP), חברות המספקות שירותים ציבוריים, וחברות בתחום החלל;
2. חברות המספקות שירותי תשתיות רשת כגון מרשמי שמות-מתחם (top-level domain name registries) וספקי שירותי DNS, בלא משמעות לגודלן;
3. חברות המספקות שירותי תקשורת אלקטרונית (service provider of electronic communication networks or publicly available electronic communications services) המעסיקות מעל 50 עובדים ושמחזור עסקיהן השנתי גבוה מ-10 מיליון אירו;
4. גופים ממשלתיים;
5. חברות שהוכרזו ככאלו שהתקנות חלות עליהן על ידי הרשויות המתאימות במדינתן, בהתאם לתקנות האירופיות השונות המאפשרות זאת.

חברות "חשובות" מוגדרות כחברות מהתחומים המנויים בסעיף 1 מעלה, אך שאינן עומדות בשאר הדרישות כדי להיחשב כחברות "חיוניות".

מהן הדרישות שמטילות תקנות NIS 2?

עיקר הדרישות והחובות שקבועות בתקנות NIS 2 הן דרישות כלפי המדינות השונות באיחוד האירופי – כגון דרישה לקבוע חקיקה לאומית מתאימה בתחומי אבטחת סייבר, הקמה של רשויות וצוותי תגובה לאומיים לאירועי סייבר, ועוד. יחד עם זאת, תקנות NIS 2 כוללות גם דרישות אשר חלות באופן ישיר על הגופים השונים הכפופים לו. בין החובות החלות על גופים אלו ניתן למנות בין היתר את החובות הבאות:

1. אימוץ תכנית ציות הכוללת נהלים בעניין ניהול סיכוני אבטחת מידע ונהלי אבטחת מידע שונים;
2. אימוץ נהלים הנוגעים להתמודדות עם אירועי אבטחת מידע (Incident Response), המשכיות עסקית, ניהול גיבויים ועוד;
3. שימוש במנגנוני אבטחה כגון MFA ואמצעי תקשורת מאובטחים, בהתאם לצורך;
4. שימוש באמצעי אבטחת מידע בסיסיים לכל הפחות, וכן עריכת הדרכות ואימונים לעובדים;
5. דיווח אודות אירועי סייבר ואבטחת מידע לרשויות הרלוונטיות במדינה בה ממוקם או פועל הגוף, בהתאם לחקיקה המקומית ולזמני הדיווח הקבועים בה;
6. לשיקול דעת המדינות השונות באיחוד, ביכולתן לדרוש מהגופים השונים הכפופים ל-NIS 2 להשתמש באמצעי אבטחת מידע אשר קיבלו את האישורים הנדרשים תחת רגולציות שונות של האיחוד האירופי.

חשוב לזכור, כי לצד חובות אלו מדינות האיחוד נדרשות כאמור לאמץ חקיקה בנושאי אבטחת סייבר העומדת בדרישות חקיקתיות של תקנות NIS 2. מדינות יכולות לבחור לאמץ בחקיקה את הסטנדרטים הקבועים בתקנות NIS 2, או להחמיר עליהן ולדרוש עמידה

בסטנדרטים מחמירים יותר ועל כן חשוב לבחון גם את החקיקה הלאומית הרלוונטית בעת בחינה של תחולת תקנות NIS 2.

מי כפוף לתקנות DORA?

תקנות DORA הן תקנות אירופאיות שמטרתן קביעת סטנדרטים להתנהלות בכל הנוגע לאבטחת מידע וניהול סיכוני אבטחת מידע במגזר הפיננסי האירופי בפרט. תקנות DORA חלות על מגוון גופים וחברות הפועלים במגזר זה, ביניהם ניתן למנות:

1. חברות אשראי;
2. ספקי שירותי תשלומים;
3. חברות המספקות שירותי השקעות;
4. ספקי שירותי נכסים קריפטוגרפיים;
5. זירות מסחר;
6. מנהלי קרנות השקעה אלטרנטיביות;
7. חברות ביטוח וביטוחי משנה;
8. מתווכי ביטוח, מתווכי ביטוחי משנה ומתווכי ביטוחים נלווים;
9. סוכנויות דירוג אשראי;
10. נותני שירותי מימון המונים;
11. ספקי שירותי אינטרנט ותקשורת (Internet Communication Technology – ICT).

כאמור, רשימה זו אינה ממצה – ועל חברות הרשומות באחת ממדינות אירופה ואשר פועלות בתחום הפיננסי לבחון האם הן כפופות לתקנות.

מהן הדרישות שמטילות תקנות DORA?

בניגוד לתקנות ה-NIS 2, במקרה של תקנות DORA, רוב החובות המנויות בתקנות מוטלות ישירות על הגופים הכפופים לחוק המפורטים מעלה ,לצד חובות המוטלות על המדינות הכפופות לתקנות לאמץ חקיקה מתאימה, ולייעד רשויות מפקחות לאומיות לצורך הפיקוח על יישום התקנות, בין היתר. בין החובות אשר חלות על הגופים הכפופים לחוק ניתן למנות את החובות הבאות:

1. אימוץ תוכניות ציות ונהלים הנוגעים לניהול סיכוני אבטחת מידע;
2. אימוץ נהלים ותהליכי עבודה אשר יבטיחו את שלמות המידע, אמינותו ונגישותו;
3. שימוש במערכות אשר יאפשרו ניטור, גילוי מוקדם של אירועי אבטחת מידע, ושמירת מידע אודות אירועי אבטחת מידע;
4. דיווח אודות אירועי אבטחת מידע לרשויות הרלוונטיות במדינה בה פועל הגוף;
5. ביצוע מבדקי חדירות (Penetration Testing);
6. בחינה וניהול של סיכוני אבטחת מידע הנוגעים לצדדים שלישיים ככלל ולספקי שירותי ICT בפרט.

נדגיש כי רשימה זו אינה רשימה ממצה, וכי גופים הסבורים כי הם כפופים לחוק נדרשים לבדוק מהן הדרישות הספציפיות החלות עליהם.

תקנות DORA עשויות כאמור לחול באופן ישיר על חברות ישראליות המספקות שירותי אינטרנט ותקשורת באירופה לגופים פיננסיים; המשמעות היא שאותן חברות, במידה ולא יעמדו בדרישות של תקנות ה-DORA, יהיו חשופות לקנסות ופיקוח מצד הרגולטורים הרלוונטיים במדינה האירופית בה הן פועלות. בנוסף, חברות ישראליות הפועלות באירופה עשויות להיתקל בתקנות ה-DORA באופן עקיף – גופים הכפופים לתקנות ה-DORA מחויבים

על פי התקנות לנהל את סיכוני אבטחת המידע הנובעים מהשימוש בספקי שירותי ICT. במסגרת כך, נדרשים הגופים לוודא כי ספקי שירותי ה-ICT שלהם משתמשים באמצעי אבטחת מידע ראויים, וכי יש להם נהלים מתאימים הנוגעים לניהול סיכוני אבטחת מידע ולהתמודדות עם אירועי אבטחת מידע וסייבר. כמו כן על הגופים הפיננסיים לכלול בהסכמים עם ספקי שירותי ICT תנאים חוזיים שונים המתייחסים בין היתר לביטול החוזה במקרים של הפרה, רמת השירות (Service Level Agreement), שיתוף פעולה עם רשויות שונות במידת הצורך ודיווח אודות אירועי אבטחת מידע וסייבר.

מדינות האיחוד השונות נדרשות תחת תקנות ה-DORA לאמץ סטנדרטיים טכניים לאבטחת מידע (הכוללים התייחסות לאמצעי אבטחת מידע ולנהלים נדרשים) עד ה-17 בינואר, 2025- אז תחל באופן רשמי התחולה של תקנות ה-DORA. סביר מאוד כי סטנדרטיים טכניים אלו יעלו כדרישה מצד הגופים הפיננסיים הכפופים לתקנות במסגרת התקשרויות חוזיות עם ספקי שירותים ככלל, וספקי שירותי ICT בפרט.

כיצד ניתן לפעול?

חברה אשר יש לה פעילות עסקית באחת ממדינות אירופה נדרשת לבדוק האם תקנות NIS 2 או תקנות ה-DORA עשויות לחול עליה, באופן ישיר או עקיף (כגון דרך דרישות חוזיות מלקוחות הממוקמים באירופה). במידה והיא סבורה כי התשובה חיובית, עליה לבחון אלו מהחובות המנויות בתקנות אלו חלות עליה, ולפעול בהקדם כדי לוודא את עמידתה בתקנות.

ככלל, אנו ממליצים לכלל לקוחותינו לערוך באופן שגרתי הערכות סיכונים בנוגע לסיכוני אבטחת מידע וסייבר בארגוניהם, ולוודא כי אמצעי אבטחת המידע שלהם, ובכלל זאת הנהלים הפנימיים של הארגון הנוגעים לאבטחת מידע ולמתן מענה לאירועי אבטחת מידע וסייבר, מספקים מענה לסיכונים האמורים.

צוות הציות במיתר ישמח לסייע בכל שאלה בנושא.

פרטי קשר

יובל ששון, שותף
ציות בינלאומי
03-6103190
ysasson@meitar.com

ד"ר שמרית איתי-חורב, שותפה
ציות בינלאומי
03-6103190
shimriti@meitar.com

נועם חורהאוס, עו"ד
ציות בינלאומי
03-6144041
noamg@meitar.com

אנו עומדים לרשותכם בכל שאלה ו/או הבהרה ונשמח לסייע בכל עניין.

למידע נוסף אודות מחלקת ציות בינלאומי במשרדנו, לחץ כאן.

להצטרפות לעדכוני לקוחות לחץ כאן

מיתר | עורכי דין
דרך אבא הילל סילבר 16, רמת גן, 5250608, ישראל | 03-6103100