ISACA Israel Chapter

כ״ד כסלו תשפ״ו, 14/12/2025

ממונה הגנת פרטיות (Data Protection Officer) בישראל – יישום הרגולציה בקו הזינוק

מאת עו״ד (MA) יוסי ברוך – CISA, CRISC, CDPSE

רקע

תפקיד ה-Data Protection Officer (להלן – **DPO** או **הממונה**) הפך בעשור האחרון מחזון ליברלי והומני אירופאי לפרקטיקה טובה ומחייבת בקהילת ה-European Union, וכפועל יוצא מכך גם בארגונים ישראליים רבים אשר פועלים בחו״ל.

במקביל, עליית המודעות הציבורית לפרטיות, תיקוני חקיקה/רגולציה מקומיים, חדירת תקני General Data Protection Regulation (להלן - **GDPR**) ודומיהם לשוק הישראלי והעולמי, ותביעות אישיות או ייצוגיות סביב שימוש במידע – כל אלה חיזקו את הצורך בגורם פנים-ארגוני שמחזיק ידע מקצועי רלוונטי, סמכות ואחריות מוגדרות בהתנהלות נכונה עם נתונים אישיים בעלי רגישות.

עם זאת, הבסיס החוקי בישראל – על אף שחוק הגנת הפרטיות, תשמ״א-1981 (להלן - **החוק**), הקדים את זמנו, הוא אינו פרטני ועדכני טכנולוגית ומסחרית כמו באירופה, ולפיכך העבודה המעשית של DPO בארץ נסמכת על שילוב בין דין מחייב, רגולציה רכה וסטנדרטים מקצועיים.

המסגרת החוקית בישראל

בניגוד ל-EU שם ה-GDPR קובע חובת מינוי DPO במצבים מסוימים, בישראל אין חובה כללית גורפת למנותו, אולם קיימים מקורות משפטיים שמעודדים ארגונים למסד תפקיד זה.

החוק עצמו אינו מתייחס לתפקיד של ה-DPO, אך מטיל על בעל מאגר מידע חובות משמעותיים - אבטחת מידע, שימוש הוגן במידע, זכויות נושאי מידע, ורישום מאגרים, אשר מינוי DPO מקצועי עשוי לספק לכך מענה מעשי נאות ליישומם.

מעל האמור, פסיקה בשנים האחרונות בתחום המשפט הפרטי והנזיקי מדגישה כי אי עמידה בחובות פרטיות עלולה להיחשב רשלנות – קרי, ה-DPO מוסיף שכבת הגנה משפטית ומנהלית לארגונו.

אמנם רוב הארגונים בישראל כיום אינם חייבים במינוי DPO על פי החוק, אולם בפועל כמעט כל גוף שמחזיק מידע רגיש, גדול או מבוזר, מגיע למסקנה מעשית שאין דרך אחרת לנהל פרטיות כהלכה.

תקנות הגנת הפרטיות (אבטחת מידע), תשע״ז–2017 (להלן - **התקנות**) מחייבות קיום מסמכי יסוד של מאגרי המידע בארגון, וכן מנגנוני תיעוד, בקרה ואכיפה של עקרונותיהם - הגדרות מאגר, תיק/תרשים אתר, ניהול רשימת הרשאות פונקציונליות תקפה, בקרת משתמשים, ניהול סיכונים. בנוסף, נדרשת אכיפת נוהל אבטחת מידע הכולל גם את שרשרת האספקה (סיכוני צד ג׳), טיפול באירוע חריג, הדרכות/מודעות עובדים ועוד.

הפעולות הללו מצויות תחת סמכות ואחריות של בעלי תפקיד שונים בארגון, ובארגונים רבים הבינו בהדרגה - מתוך צורך תפעולי, חשש משפטי או דרישות סקטוריאליות - כי ליישום אחיד ופיקוח באופן חוצה ארגון של חובות הגנת הפרטיות נדרש בעל מקצוע ייעודי.

תיקון 13 לחוק שהוחל מ-6/8/2024 (להלן - **התיקון**) שינה את התמונה בקבעו, כי במאגרים מסוימים, ובפרט במאגרי מידע שחובה לרושמם, על בעל המאגר למנות DPO – זאת בעיקר ביחס לגופים המחזיקים במאגרים מהותיים או רגישים:

- בעל שליטה או מחזיק במאגר מידע שהוא גוף ציבורי כהגדרתו בסעיף 23(2) לחוק;
- בעל שליטה במאגר מידע שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, ...דיוור ישיר, ויש במאגר מידע אישי על יותר מ־10,000 בני אדם;
- בעל שליטה או מחזיק במאגר מידע שעיסוקיו העיקריים כוללים פעולות עיבוד מידע או כרוכים בפעולות כאמור, אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר, ...ספק מורשה המספק שירות רדיו טלפון נייד לפי חוק התקשורת (בזק ושידורים), תשמ״ב-1982 וספק שירות חיפוש מקוון או מי שעיסוקו העיקרי כרוך בפעולות אלה;
- בעל שליטה או מחזיק במאגר מידע או מחזיק במאגר מידע שעיסוקו העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר - תאגיד בנקאי (כהגדרתו בחוק הבנקאות (שירות ללקוח) תשמ״א-1981, מבטח (כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ביטוח) תשמ״א-1981, בית חולים כללי (כהגדרתו בפקודת בריאות העם 1940), וקופת חולים (כהגדרתה בחוק ביטוח בריאות ממלכתי תשנ״ד-1994).

התיקון אף הגדיר מהותית את תפקידיו של ה-DPO בסעיף 17ב2.(א) – לפעול להבטחת קיום הוראות החוק על ידי בעל השליטה או המחזיק, ולקידום השמירה על הפרטיות ואבטחת המידע במאגרי המידע:

- ישמש סמכות מקצועית ומוקד ידע - ייעץ להנהלת הגוף שהוא ממלא בו את תפקידו ולעובדיו, יכין תוכנית הדרכה ויפקח על ביצועה.
- יכין תוכנית לבקרה שוטפת על העמידה בהוראות החוק לגבי מאגרי מידע - יוודא את ביצועה על ידי בעל השליטה או המחזיק במאגר המידע, ידווח להנהלת הגוף שהוא ממלא בו את תפקידו על ממצאיו ויציע הצעות לתיקון הליקויים.
- יוודא את קיומם של נוהל אבטחת מידע ומסמך הגדרות המאגר - שעריכתם נדרשת בהתאם לתקנות לפי סעיפים 17(ב) ו-36 לחוק, שיובאו לאישור הנהלת הגוף שבו הוא ממלא את תפקידו.
- יוודא טיפול בפניות של בני אדם שמידע אישי על אודותיהם נמצא במאגר המידע - לגבי עיבוד מידע כאמור או מימוש זכויותיהם לפי חוק זה, ובכלל זה בקשות לעיון במידע אישי או לתיקונו (דרכי ההתקשרות עמו יפורסמו לציבור באופן נגיש ופשוט);
- ישמש איש קשר לרל״פ - עבור הגוף שבו הוא ממלא את תפקידו.

הלכה למעשה, במגזרים רבים בישראל הפך ה-DPO מנדטורי, ואצל רבים אחרים הוא הפך סטנדרט מקצועי שאי אפשר להתעלם ממנו – בתיקון נקבעו גם התנאים להפעלתו ומהם כישוריו הנדרשים:

- בעל השליטה או המחזיק במאגר המידע יספקו לממונה את התנאים והמשאבים הדרושים למילוי נאות של תפקידו ויוודאו שהוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות.
- הממונה ידווח ישירות למנכ"ל של בעל השליטה או המחזיק במאגר המידע, או לעובד שכפוף ישירות אליו.
- כישורי הממונה למילוי תפקידו באופן נאות לפי סעיף 17ב3.(א) לחוק:
  - בעל הידע והכישורים הנדרשים, ובכלל זה ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע והיכרות עם תחומי פעילותו של הגוף שבו הוא ממלא את תפקידו ומטרותיו, בשים לב לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו.
  - יכול שיהיה מי שאינו עובד הגוף שבו ימלא את תפקידו.
  - לא ימלא תפקיד נוסף ולא יהיה כפוף לנושא משרה בגוף שבו הוא ממלא את תפקידו או בגוף אחר, אם מילוי התפקיד או הכפיפות כאמור עלולים להעמידו בחשש לניגוד עניינים.

מעל האמור, קיימות חובות נוספות המעצבות את התפקיד במסגרת תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 – אלה מחייבות נהלים, בקרות, בדיקות תקופתיות, הדרכות וניהול אירועים חריגים, כל זאת באופן המצריך גורם מקצועי אחראי כאשר במרבית המקרים, מינוי ממונה פרטיות הוא הדרך המעשית לעמוד בדרישות.

בנוסף ישנה רגולציה סקטוריאלית, המחזקת מגמה זו:

- בנק ישראל מחייב תהליכי אבטחת מידע קפדניים.
- רשות שוק ההון דורשת זיהוי וניהול סיכוני מידע.
- משרד הבריאות דורש הגנה על מידע רפואי רגיש בהנחיות או בתקנים ייעודיים - מוסדות רפואיים נדרשים לעמידה בהוראות חוק זכויות החולה וחוזרי משרד הבריאות.

<u>החלת GDPR על חברות ישראליות</u>

חברות הפועלות מול אירופה או המבצעות עיבוד נתונים של תושבי ה-EU נדרשות למנות DPO לפי הדירקטיבה האירופית, וכך התפקיד מיובא לישראל גם ללא חובה מקומית.

מ-DPO בחברה מסוג זה נדרשים ידע ואחריות משפטית ורגולטורית המאפשרים יישום יומיומי של שיטות/נהלים ואמצעים/טכנולוגיה אפקטיביים, בין היתר:

- חוק הגנת הפרטיות לרבות תיקון 13, והתקנות מכוחו.
- הנחיות הרשות להגנת הפרטיות
- ה-GDPR והגדרות/החלטות של ה-EDPB - ביחס לתאימות (Adequacy) בינלאומיות של רמת אבטחת המידע במדינות מחוץ לאיחוד אשר פועלות מול גורמים בתוכו, או סעיפים הסכמיים המסדירים זאת ביחס לאחסון/עיבוד נתונים, העברה ושיתוף מידע.

מה-DPO נדרשת כיום בפועל גם הבנה טובה טכנולוגית ותפעולית, מכיוון ואחריותו מקיפה את אלה:

- בחינת פיתוח, ניהול ובקרת מערכות מידע – לרבות שיטה ואמצעים לגיבוי/שחזור נתונים ואמצעי בקרה והגנת מידע וסייבר.

- ניהול ובקרת משתמשים והרשאות, כולל - באמצעות הליכי משא"ן (כגון סינון כ"א או חתימת NDA), ניטור LOGS ובדיקה תקופתית למול מדיניות/נוהלי הארגון.
- וידוא ביצוע סקרי סיכונים, PIA/BIA, מבדקי חדירה ו-Phishing/הנדסה חברתית.
- טיפול נאות באירועי מידע – לרבות תחקיר והפקת לקחים.
- שיתוף פעולה שוטף עם CIO/מנמ"ר, CISO, DEVOPS, PMO, CRO/ממונה המשכיות עסקית וכיו"ב.
- וידוא יעוץ משפטי וטכני נאות להבניית ממשל ניהול ובקרה אפקטיביים של הגנת מידע/סייבר ופרטיות מול ספקים (צד ג') – החל בעריכת הסכם ומפרט התקשרות עמם וכלה בביצוע ביקורת בחצרות הספק.

דגשים בפסיקה רלוונטית ועדכנית

הגנת הפרטיות מהווה זכות יסוד המוגנת בדין הישראלי ומתבטאת במספר הקשרים משפטיים, הבאה לידי ביטוי בהליכים פליליים, בהגנה על נפגעי עבירה, בהגבלת מסירת חומרי חקירה, ובאיזון מול אינטרסים אחרים כגון פומביות הדיון – קיומו של DPO אפקטיבי עשוי להביא ערך רב לארגונו במניעת תביעות משפטיות או פגיעה בשם הטוב, מאחר ומעצם מילוי תפקידו כהלכה הוא יוצר עבורו הסדרה בשיטת ואמצעי הבקרה והניהול של מידע אישי או בעל רגישות במאגרי המידע.

יודגש, כי החקיקה הישראלית מעגנת את ההגנה על הפרטיות בחוקים שונים, ובתי המשפט מפרשים ומיישמים הגנות אלו תוך איזון מול זכויות וערכים אחרים, יותר ויותר ככל שהחקיקה הועמקה והאכיפה חוזקה – להלן מספר דוגמאות של מקרים מייצגים, כלליים ופרטיים :

- בהליכים פליליים העוסקים בעבירות מין - קיימת הכרה מיוחדת בצורך להגן על פרטיותם של המעורבים. החוק מאפשר לבית המשפט להורות על סגירת דלתיים לשם הגנה על עניינו של מתלונן או נאשם בעבירת מין או בעבירה על פי החוק למניעת הטרדה מינית. מטרת ההגנה היא למנוע פגיעה קשה בצנעת הפרט העלולה להיגרם להם כתוצאה מההליך הפלילי, במיוחד לאור העובדה שעבירות אלה כרוכות בדרך כלל בחשיפת פרטים אינטימיים ביותר. ישנו חשש מוכר כי פרסום שמו של נאשם, אף ללא פרטים מזהים של המתלונן, עלול להוביל לחשיפת זהות המתלונן ולפגיעה בפרטיותו בקרב אנשים שעשויים לזהות אותו.
- איזון בין הזכות לפרטיות לבין זכות העיון בחומרי חקירה - קיים מתח מובנה בין זכות הנאשם לעיין בחומרי חקירה לבין ההגנה על פרטיותם של צדדים שלישיים. בבחינת בקשות לעיון בחומרי חקירה, יש לבחון את התועלת שבמסירת המידע אל מול עוצמת הפגיעה בפרטיות. ככל שהתועלת הצפויה לנאשם מעיון בחומר פחותה והפגיעה בפרטיותו של צד שלישי משמעותית יותר, כך תגבר הנטייה שלא לאפשר לנאשם לעיין בחומר. המבחן המשפטי מחייב איזון בין האינטרסים השונים, כאשר קיומה של פגיעה ממשית בפרטיות של אדם מהווה שיקול משמעותי נגד מסירת המידע. כמו כן, חומרי חקירה הכוללים מידע פרטי הנוגע לנחקר מהווים סוג של מידע שאין הכרח להורות על העברתו לעיון הנאשם.
- הגנת פרטיות במסגרת חקירות פליליות - מתעוררת שאלת הזכות לקבלת חומרי חקירה על ידי צדדים שאינם הנאשם עצמו. המשפט הישראלי מבחין בין זכותו של נאשם לקבל חומרי חקירה לפי סעיף 74 לחוק סדר הדין הפלילי, לבין זכויותיהם של צדדים אחרים. גם במקרים בהם מוגש כתב אישום נגד חשוד, אין בכך כדי להקנות לצדדים שלישיים (כגון נפגעי עבירה) זכות אוטומטית לקבלת חומרי החקירה. הגבלה זו נועדה, בין היתר, להגן על פרטיותם של המעורבים בהליך החקירה, ובמיוחד על פרטיותו של החשוד או הנאשם.

- פגיעה בפרטיות מוכרת בחוק הישראלי כעבירה פלילית - בהקשר של עבירות מין, חוק הגנת הפרטיות (התשמ"א-1981) קובע בסעיפים 2(3) ו-5 עבירה של פגיעה בפרטיות. עבירה זו עשויה להתקיים לצד עבירות אחרות כמו עבירות מין, הטרדה מינית או פרסום והצגת תועבה. המחוקק רואה בפגיעה בפרטיות ערך מוגן שיש להגן עליו באמצעות המשפט הפלילי, במיוחד כאשר הפגיעה משולבת בעבירות אחרות הפוגעות בכבוד האדם ובאוטונומיה שלו.
- הגנת פרטיות של קטינים בהקשר של עבירות מין ופורנוגרפיה - החזקת פורנוגרפיית קטינים נתפסת לא רק כפגיעה בקטינים הספציפיים המצולמים, אלא כפגיעה בכבודם, בפרטיותם, ובשלמות גופם ונפשם של קטינים באופן כללי. זאת מאחר שצריכת תמונות וסרטונים כאלה עלולה לעודד את המשך ייצורם הפוגעני. החזקת חומרים כאלה עלולה לשמש את המחזיק לשידול קטינים אחרים להצטלם באופן דומה, ואף להביאו לנסות ולחקות את המעשים המוצגים בהם תוך פגיעה בילדים נוספים. המשפט מכיר בחומרה היתרה של פגיעה בפרטיות קטינים בהקשרים אלה.
- המגן לחופש הפרט ע"ר נ. מנכ"ל משרד הבריאות (בג"ץ 5822/21, עליון) - העותרת טענה כי מסירת מידע אנונימי על בני נוער מחוסנים לחברת פייזר מפרה את זכותם לפרטיות. בית המשפט העליון החליט שלא יתערב בשיקול הדעת המקצועי של גורמי הממשלה והכנסת בנוגע להתמודדות עם מגפת הקורונה, אלא במקרים חריגים של פגם היורד לשורש העניין, כגון שיקולים זרים או אי-סבירות קיצונית. בית המשפט מדגיש כי הוא אינו שם עצמו בנעלי הרשויות המינהליות המוסמכות ואינו מחליף את שיקול דעתן, במיוחד בסוגיות שבמומחיות רפואית.
- West Face Capital inc corporation נ. חיות גרינברג ,עו"ד מנהלת מיוחדת והכנ"ר (ע"א 4891/20, עליון) – ביחס להגנת פרטיות על מידע עסקי וסודות מסחריים של צדדים שלישיים במחשבי חברה בפירוק נקבע, שבנוסף לחיסיון הספציפי שחל על גופים חדלי פירעון, חל גם חיסיון כללי מכוח סעיף 23ב לחוק, הקובע שלגוף ציבורי (המשיבים בעתירה) אסור למסור מידע, "זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על פי סמכות כדין, או שהאדם אשר המידע מתייחס אליו נתן הסכמתו למסירה". בית המשפט בחן אם בקשת העיון הולמת את סעיף 8(א) לחוק העזרה המשפטית, הקובע כי "פעולה בישראל על פי בקשה לעזרה משפטית של מדינה אחרת, תיעשה בדרך שנעשית פעולה מסוגה בישראל, ויחולו עליה הוראות הדין החלות בישראל על פעולה מסוגה, אלא אם כן נקבע אחרת בחוק זה או על פיו". נקבע כי הפעולה המבוקשת אינה עולה בקנה אחד עם הדרך שבה נעשית פעולה מהסוג המבוקש בישראל.

<u>תרבות ופרקטיקה ארגונית</u>

האתגר של DPO הוא לשנות מודעות והרגלי עבודה בארגון, עליו לשמש שגריר של מקצועיות, הוגנות ושיקול דעת במימוש עיצוב לפרטיות, שקיפות, תכליתיות ומידתיות בשימוש במידע – לשם כך עליו לאחוז גם במיומנויות בין-אישיות רכות לא פחות מטכנולוגיות או משפטיות.

חרף האמור, כיום עדיין קיים פער בין הוראות החוק/רגולציה לבין הפרקטיקה הנוהגת בארגונים, למרות הרחבת סמכויות ואמצעי האכיפה ואחריות הנהלה ודירקטוריון בתיקון 13 לחוק. בפועל ארגונים רבים מתקשים לאתר ממונה בעל מכלול הכישורים המתאימים ומוצאים תחליף חלקי – איש IT או יועמ"ש אשר להם מגבלה בגישה למידע ובעלי תפקיד חיוניים וחוסר עצמאות מול ההנהלה:

- בעל תפקיד במעמד זוטר יותר בהיררכיה הארגונית – סמכות ואחריות נמוכות יותר.
- הקצאת משאבים חומריים פחותה – תקציב, תקן, הכשרה מקצועית, אמצעים טכנולוגיים וכיו"ב.

- ריבוי תפקידים יוצר עומס, ועלול לגרום לניגוד עניינים מקצועי או אתי.
- שיתוף נמוך בידיעה ומעורבות של הממונה בשלבי תכנון מוקדמים של מדיניות, תהליכים ומערכות בארגון (מונע יישום Privacy by Design).
- התוצאה - מינוי רשמי שאינו מגובה בתפקוד מקצועי נאות, למעשה עלה תאנה של פרטיות לארגון.

סיכום – מגמה ותחזית

הגדלת סמכויות ואמצעי והאכיפה, בתחום האזרחי והפלילי כאחד, של הרשות להגנת הפרטיות בתיקון 13 לחוק לאחרונה צפוי להגדיל את היקף ועומק פעילותה במידה ניכרת - דרישות שקיפות ודיווח מדויק ובמועד, ריבוי ביקורות במוקדי הסיכון (ארגונים פיננסיים, רפואיים, הסוחרים במידע/דיוור ישיר וכדומה), אכיפה מוגברת של אחריות מנהלים ובעלים. במקביל מוערך, כי עליית המודעות לפרטיות והחמרת הסנקציות (בפרט אפשרות הפיצוי ללא צורך בהוכחת נזק) בגין הפרתה תגרור ריבוי תלונות מנהליות ותביעות משפטיות כנגד מוסדות וחברות מסחריות מצד הציבור.

להערכת הכותב, ה-DPO יהפוך בהדרגה בשנים הקרובות לנקודת הממשק העיקרית של ארגונו, הן מול הרשות והן מול הציבור, לפיכך – יש חשיבות רבה בשכלול מסגרת התפקיד ומיומנויות הממונה, אשר צפוי כי יישא אופי היברידי בתחומים המשפטי, הטכנולוגי, המנהלי/תפעולי והתקשורתי (טיפול באירועי אבטחה/פרטיות חריגים ושמירה על מוניטין הארגון).

בנוסף ניכרת עלייה ברף הציפיות העסקיות מצד שותפים, לקוחות וספקים – כולם מצפים יותר ויותר לממשל תאגידי שוטף של פרטיות ולמענה מאחראי מקצועי, בדומה לפרקטיקה הטובה כיום ב-EU.

תיקון 13 מסמן שינוי משפטי ומעשי חשוב – הממונה בישראל הפך מפרקטיקה וולונטרית לחובה רגולטורית, שנדרש בניהול ובקרה אפקטיביים של מאגרי המידע בארגונים רבים. עם זאת, הגדרת הצורך והמסגרת למימוש תפקיד זה עדיין מתעצבת, כדי לשלב בין דינים מקומיים שחלקם מיושנים וכלליים לבין מתודולוגיות עדכניות של ניהול הגנת פרטיות ומידע/סייבר בעולם דיגיטלי ואינפורמטיבי.

המבחן המעשי של ארגון אינו רק במינוי הפורמלי של DPO, אלא ביציקת תוכן ומשאבים מהותיים לתפקיד שיאפשרו ביצוע אפקטיבי שלו – על מנת שיספקו לארגון על עובדיו, לקוחותיו וספקיו מענה איכותי לשמירה על חיסיון המידע האישי שלהם, כמו גם על הסוד המסחרי שלו.

ביבליוגרפיה

- חוק הגנת הפרטיות, תשמ"א–1981 (כולל תיקון מס' 13, אוגוסט 2024).
- תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז–2017.
- חוק זכויות החולה, תשנ"ו-1996.
- סקירת פסיקת בתי משפט בתחום "הגנת פרטיות" בכל הערכאות (2021-2025) – סיכום AI באמצעות אתר "דינרגע" (https://www.dinrega.com).
- הרשות להגנת הפרטיות במשרד המשפטים (שנים שונות) - הנחיות מקצועיות, מסמכי מדיניות, דוחות ביקורת ועמדות רשמיות.

- European Union. (2016). General Data Protection Regulation (EU 2016/679). Official Journal of the European Union.
- International Organization for Standardization. (2019). ISO/IEC 27701: Security techniques — Extension to ISO/IEC 27001 and 27002 for privacy information management.
- בנק ישראל (שנים שונות) – הנחיות נב"ת לניהול סיכוני סייבר ואבטחת מידע.
- רשות שוק ההון (שנים שונות) - הוראות ניהול סיכוני מידע ואבטחת נכסים דיגיטליים.
- משרד הבריאות (שנים שונות) - חוזרים ונהלים בנושא מידע רפואי, אבטחת מידע ופרטיות.
- European Data Protection Board (EDPB). (שנים שונות). Guidelines on Data Protection Officers, Roles and Responsibilities.
- מאמרי מדיניות, ספרות אקדמית וניתוחים בתחום הגנת הפרטיות בישראל ובעולם העוסקים בהשפעת GDPR, רגולציה מקומית ויישום תפקידי DPO בארגונים.