



חובת מינוי ממונה על הגנת פרטיות בארגונים (DPO) ואיפיון התפקיד:

סקירה והמלצות

מנחי הקליניקה לפרטיות: פרופ' מיכאל בירנהק, עו"ד נועה דיאמונד

והסטודנטים אסף ניאזוב, אלה שרק, שנה"ל תשפ"ד

מאי 2024

תקציר

צמיחתו של תחום הגנת המידע בעקבות התפתחות הטכנולוגיה, איסוף ועיבוד הנתונים בכמות נרחבת, לווה בהכרה שיש לפעול בדרכים שונות להגן על האינטרסים של נושאי המידע. כחלק ממגמה זו, הוכרה החשיבות של ייחוד תפקיד בארגונים לצרכי הגנה על פרטיות במידע. מינוי וולונטרי של ממונה על הגנת הפרטיות במידע (DPO) נפוץ ברחבי העולם, ובפרט באיחוד האירופי. המינוי הומלץ באופן וולונטרי בדרך של Best-Practice גם על-ידי הרשות להגנת הפרטיות בישראל, בשנת 2022. עם תחילת היישום של רגולציית ההגנה על המידע (GDPR) באיחוד האירופי, מינוי זה הפך לחובה במדינות אירופה. לעמדת הקליניקה לפרטיות, נכון לקבוע חובת מינוי כזו גם בדין הישראלי, במקרים המתאימים, שיוגדרו בהתחשב בהיקף ורגישות המידע הנאסף בארגון. על קביעת החובה להתבצע תוך איזון בין שאיפה להגנה מירבית על פרטיות למניעת הטלת עומס בלתי סביר על ארגונים.

מאחר שעברו מספר שנים מתחילת חובת המינוי באיחוד האירופי, ניתן להבחין בהשפעות של חובה זו על השוק בפועל. סקר שערך האיחוד האירופי מצא פערים אכיפתיים משמעותיים – ארגונים שנדרשו בחוק למנות DPO לא עשו זאת, לא ניתנו ל-DPO משאבים מתאימים, מונו DPOs שמחזיקים במקביל בתפקידים שמציבים אותם בניגוד עניינים וכן DPOs לא היו מעורבים בצורה מספקת בקבלת ההחלטות בארגון.

← ניתן ורצוי ללמוד מהניסיון האירופי ובהחלטות לגבי יישום חובת מינוי DPO בישראל יש לתת את הדעת על הפערים הללו, תוך התחשבות בייחודיות של השוק הישראלי כשוק קטן יחסית.

תפקידי ה-DPO מגוונים, וכוללים בעיקר פיקוח על ציות לחקיקה הקשורה לפרטיות ולרגולציה הקשורה להגנה על מידע אישי, התווית מדיניות הארגון בנושא עיבוד מידע אישי, גיבוש תסקיר השפעה על פרטיות בארגון, שיתוף פעולה עם הרשות המאסדרת ותפקוד כאיש קשר של הרשות המאסדרת ונושאי המידע בענייני עיבוד מידע.

← אנחנו סבורים שיש להגדיר תפקידים אלו בחוק כתפקיד מובחן מממונה אבטחת מידע בארגון.

← בנוסף אנו סבורים שכדי לאפשר מילוי תפקידיו באופן מהותי, יש לעגן בחקיקה מנגנונים שונים שיבטיחו את רמת כישוריו ושימור כשירותו של ממונה הגנת הפרטיות, עצמאותו, היעדר ניגוד עניינים ומיקומו בתוך המערך הארגוני.

← בנוסף, כדי להעניק לתפקיד את החשיבות הראויה לו, נמליץ להתייחס להיבטים של אחריות הממונה ולקבוע סנקציות במקרה של אי-ציות.

מבוא

אחד ממניעי תיקון 14 לחוק הגנת הפרטיות הוא "השינויים הטכנולוגיים והמשקיים מרחיקי הלכת באופן שבו מידע נאסף, מעובד ונעשים בו שימושים נוספים, וזאת במסגרת הפעילות השגרתית של ארגונים ויחידים." מטרת ההצעה היא להתאים את החוק לאותם אתגרים עכשוויים בהגנה על מידע אישי במאגרי מידע.¹ כחלק מאותה מגמת עדכון, הקליניקה לפרטיות סבורה שיש לנקוט צעדים נוספים על מנת להתאים את החוק לעולם המודרני. נייר עמדה זה דן באמצעי שלטעמנו הוא בעל פוטנציאל משמעותי למנוע מראש גישה ושימוש לא נכון במידע אישי: הטמעת תפקיד ה-DPO (Data Protection Officer) מרגולצית ההגנה על המידע (GDPR) באיחוד האירופי, בחוק בישראל כממונה הגנה על הפרטיות.

מינוי וולונטרי של ממונה הגנת הפרטיות במידע נפוץ ברחבי העולם, ובפרט באיחוד האירופי. המינוי הומלץ באופן וולונטרי בדרך של Best-Practice על-ידי הרשות להגנת הפרטיות בישראל בשנת 2022. עם כניסת ה-GDPR לתוקף מינוי זה הפך לחובה במדינות אירופה. מגמה זו מתבססת על תפיסה לפיה תפקיד ה-DPO נחוץ לצורך הגנה על פרטיות המידע, בעידן גלובלי שבו נתונים אישיים זורמים באופן חסר תקדים וחוצה גבולות. בנייר עמדה זה, אנו ממליצים לחייב מינוי זה בחקיקה, ומציעים כיצד להגדירו ולאפיינו.

בפרק הראשון נתאר כיצד בא לעולם תפקיד ה-DPO ומדוע הוא נחוץ. נציג כיצד התפקיד בא לידי ביטוי ב-GDPR, ומה הוא כולל, כדי ליצור תשתית להבנת התפקיד והמשך הדיון. **בפרק השני** נציג את התוצאות בשטח, כיצד התפקיד מיושם בפועל באיחוד האירופי ובפרט את הקשיים שעולים מהגדרת התפקיד בצורתו הנוכחית באירופה. זאת כדי שנוכל להבין אלו עקרונות ראוי לאמץ מהדין האירופי ומה נרצה להטמיע בצורה משודרגת. **בפרק השלישי** נציג את הדין הקיים בישראל כתשתית להבנה כיצד ניתן להטמיע את התפקיד לדין הישראלי. **בפרק הרביעי** נציע כיצד ניתן להטמיע בישראל את תפקיד ממונה על הגנת הפרטיות, ובעיקר מהם השיקולים שיש לתת עליהם את הדעת הן בראי האתגרים שתיארנו בפרק השני והן לאור ייחודיות הדין הישראלי. בסוף פרק זה מרוכזות המלצותינו. לבסוף **נסכם**.

1.1 Data Protection Officer – רקע ונחיצות

תחום הגנת המידע הלך וצמח בעקבות התפתחות הטכנולוגיה שאפשרה תהליכי איסוף ועיבוד נתונים בכמות נרחבת, ובעקבות תהליכי גלובליזציה שהפנו את המבט לבחינת זרימת נתונים אישיים באופן חוצה גבולות. מכאן עלה צורך להגן על האינטרסים של נושאי המידע ועם זאת לאפשר את זרימת הנתונים.² הדבר נעשה תחילה דרך משפט רך: נוצרו נהלי מידע הוגן (FIPs) על ידי ההמלצות של ה-OECD והאמנה של מועצת אירופה (CoE), ובהמשך, הדירקטיבה המחייבת של האיחוד האירופי משנת 1995.³

¹ דברי ההסבר להצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022, ה"ח הממשלה 1496, https://fs.knesset.gov.il/24/law/24_ls1_615961.pdf

² Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMP.L.& SECURITY REPORT 508, 513-514 (2008).

³ Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ L281, 23.11.1995, p.31).

הדירקטיבה קבעה את כללי המשחק בעולם הגנת הפרטיות וחייבה את המדינות החברות באיחוד לקבוע חוקים לאומיים שיבטיחו את היישום המלא של ההוראה,⁴ וכן כללה תחולה גם על מדינות מחוץ לאיחוד האירופי אשר זורמים אליהן נתונים אישיים מאירופה.⁵

בשנת 2001 אימץ האיחוד האירופי רגולציה שפירטה והוסיפה להוראות הדירקטיבה בכל הנוגע להבטחת הגנה בעיבוד נתונים אישיים על ידי גופים ומוסדות, והרחיבה את סמכויות הרשויות המפקחות שאחראיות להבטחת ציות לרגולציה.⁶

כלומר, השמירה על כללי המשחק נהפכה למורכבת יותר. לחברות גלובליות גדולות נוסף האתגר להבין מהו הדין שחל עליהן, וכיצד עליהן ליישם את התקנות והרגולציה כדי לשמור על התאימות הנדרשת לאורך כל מחזור איסוף ועיבוד הנתונים שהן מבצעות. חברות קטנות יותר גם התמודדו עם אתגרי ציות ובעיקר השקעה של משאבי טכנולוגיה ומשאבים משפטיים כדי להתמודד עם מורכבות הציות לתקנות והרגולציה.⁷

כמענה לקשיים הללו, הרגולציה מ-2001 הציגה את תפקיד ה- (DPO) Data Protection Officer. לפי הרגולציה, על הגופים למנות גורם שימש עבורם כ-DPO בארגון שיבטיח יישום התקנות והרגולציה הנדרשות, שיהיה בקשר עם הרשויות המפקחות, ויסייע לבעל השליטה במידע (Data Controller) ולמעבד המידע (Data Processor) בארגון לבצע את עבודתם תוך שמירה על זכויות נושאי המידע (Data Subjects). כדי שה-DPO יבצע את עבודתו כראוי, נקבע שיש לוודא שהוא ממונה על סמך הידע המקצועי שלו ושעבודתו תעשה באופן עצמאי ונטול ניגוד עניינים.⁸

התפתחויות טכנולוגיות נוספות, בפרט התפתחותו של האינטרנט והפיכתו לפלטפורמה מרכזית לאיסוף מידע, הובילו לאיסוף מידע בהיקף חסר תקדים. לעמדת האיחוד האירופי, איסוף מידע שכזה, כאשר אינו מוסדר, עלול לפגום באמון הצרכנים בשוק ולהרתיע פעילות כלכלית.⁹ על רקע זה נכנס לתוקף ב-2018 ה-GDPR של האיחוד האירופי, במסגרתו הורחב תפקיד ה-DPO והוגדרו בהרחבה סמכויותיו, עצמאותו והעקרונות שעליו לעמוד בהם.¹⁰

⁴ סעיף 24 לדירקטיבה 95/46.

⁵ סעיף 25 לדירקטיבה 95/46.

⁶ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.01.2001, p. 1)

⁷ [Stephen J. Bigelow & Ben Cole, Privacy Compliance, TECH TARGET, https://www.techtarget.com/searchcio/definition/privacy-compliance](https://www.techtarget.com/searchcio/definition/privacy-compliance)

⁸ סעיף 24 לרגולציה 45/2001.

⁹ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0011%3AFIN>

¹⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1-88), <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (להלן: GDPR).

1.1 תפקיד ה-DPO תחת ה-GDPR

החובה למנות DPO

ה-GDPR מחייב גופים מסוימים שעליהם חלה הרגולציה למנות DPO. זאת, בין היתר, כאשר עיבוד המידע מתבצע על ידי גוף ציבורי, פרט לבתי משפט;¹¹ כאשר פעולות הליבה של הארגון כוללות עיבוד מידע אישי ואשר מתוקף טיבו, היקפו או מטרותיהן, מחייבות ניטור שיטתי ומערכתי של נושאי מידע בהיקף רחב;¹² או כאשר ליבת העיסוק של הארגון כוללת עיבוד מידע אישי רגיש בהיקף רחב.¹³ בגופים ציבוריים יכול להתמנות DPO יחיד למספר גופים, בהתחשב בגודלם ובמבנה הארגוני שלהם.¹⁴ מספר חברות קשורות (group of undertakings), אשר לאחת מהן שליטה על עיבוד המידע האישי באחרות, יכולות גם הן למנות DPO יחיד, בתנאי שה-DPO נגיש בקלות לכולן.¹⁵ ה-DPO יכול להיות שכיר בארגון או מינוי חיצוני בהתאם לחווה שיופקד אצל הרשות המאסדרת.¹⁶

תפקיד ה-DPO

משימות הממונה על הגנת הפרטיות כוללות ייעוץ בנוגע ליישום החובות המנויות ב-GDPR ובחוקים אחרים של האיחוד האירופי או של המדינה הרלוונטית, בנושא הגנה על מידע אישי;¹⁷ פיקוח על ציות הארגון לרגולציה בנושא הגנה על מידע אישי ועל מדיניות הארגון בנושא;¹⁸ הקצאת אחריות לבעלי התפקידים הרלוונטיים, העלאת מודעות והדרכת העובדים; ייעוץ ופיקוח על תהליך גיבוש תסקיר השפעה על פרטיות בארגון;¹⁹ שיתוף פעולה עם הרשות המאסדרת;²⁰ ותפקוד כאיש הקשר של הרשות המאסדרת בענייני עיבוד מידע.²¹ על ה-DPO להתחשב בעת מילוי תפקידו בסיכונים הכרוכים בפעילות עיבוד המידע, תוך התחשבות באופי, בהיקף, בהקשר ובמטרות העיבוד.²²

כשירות לתפקיד

לפי ה-GDPR, ממונה ההגנה על הפרטיות נדרש להיות בעל מומחיות בדינים ובנהלים העוסקים בהגנה על מידע אישי.²³ רמת המומחיות הנחוצה והידע צריכים להיקבע על בסיס הליכי העיבוד וההגנה הנדרשת על

¹¹ סעיף 37(1)(a) ל-GDPR.

¹² סעיף 37(1)(b) ל-GDPR.

¹³ סעיף 37(1)(c) ל-GDPR.

¹⁴ סעיף 37(3) ל-GDPR.

¹⁵ סעיף 37(2) ל-GDPR.

¹⁶ סעיף 37(6) ל-GDPR.

¹⁷ סעיף 39(1)(a) ל-GDPR.

¹⁸ סעיף 39(1)(b) ל-GDPR.

¹⁹ סעיף 39(1)(c) ל-GDPR.

²⁰ סעיף 39(1)(d) ל-GDPR.

²¹ סעיף 39(1)(e) ל-GDPR.

²² סעיף 39(2) ל-GDPR.

²³ סעיף 37(5) ל-GDPR.

הנתונים המסוימים בחברה.²⁴ רמת המומחיות הנדרשת לא מוגדרת בפירוט, אך היא צריכה להיות תואמת את הרגישות, המורכבות וכמות הנתונים שהארגון מעבד.²⁵

עצמאות

תחת ה-GDPR, ה-DPO צריך להיות עצמאי בפעילותו - אין להנחות אותו ביחס לפעילותו, ואין לפטר אותו או לפגוע בתנאי העסקתו בשל ביצוע תפקידיו.²⁶ עם זאת, האוטונומיה שה-DPO מקבל לא מקנה לו סמכות לבצע משימות מעבר למוקנה לו מכוח סעיף 39. יתרה מכך, האחראים לעמידה בחוק הם בעל השליטה במידע ומעבד המידע אשר יכולים להתנגד להמלצת ה-DPO. במקרה כזה יש לאפשר ל-DPO להציג את עמדתו מול הנהלה בכירה יותר.²⁷

ה-GDPR לא קובע פרוצדורה לפיטורים או החלפה של DPO, זאת בניגוד לרגולציה מ-2001. הגוף המייעץ לענייני הגנת מידע ופרטיות באיחוד האירופי (להלן: "הגוף המייעץ") המליץ שבחזרה של ה-DPO יהיו ערבויות נגד פיטורים לא הוגנים, זאת גם כדי לקדם את עצמאות ה-DPO בפעולותיו.²⁸

בגרמניה בחר המחוקק להרחיב את עצמאותו של ה-DPO, וקבע שלא ניתן להפסיק את העסקתו של DPO אלא במקרים שבהם לא ניתן לצפות באופן סביר מהמעסיק להמשיך את העסקתו.²⁹ הגבלה זו יוצרת העדפה למינוי DPO לזמן קצוב או מינוי DPO חיצוני.³⁰ בית הדין לצדק של האיחוד האירופי (ECJ) נדרש לבחון את התאמתו של החוק הגרמני ל-GDPR, וציין כי ייתכנו מקרים שבהם עצמאות רבה מדי תפגע בהגנה על המידע בארגון ובתכלית החקיקה. לדוגמה, כאשר ה-DPO כלל אינו מוסמך למלא את תפקידיו, או כאשר מתגלה כי הוא מצוי בניגוד עניינים.³¹

ניגוד עניינים

על פעולותיו של ה-DPO חל חיסיון או סודיות, בהתאם להקשר.³² ה-DPO יכול למלא תפקיד אחר בארגון, אך על החברה חובה להימנע מניגוד עניינים במסגרת פעילותו.³³ התפקידים שביצועם במקביל מעיד על ניגוד עניינים אינם מוגדרים ב-GDPR, וניגוד העניינים ייקבע בהתאם להקשר. עם זאת נקבע כי DPO לא יכהן

²⁴ Recital 97 ל-GDPR.

²⁵ Article 29 data protection working party, *Guidelines on Data Protection Officers ('DPOs')*, p. 12, <https://ec.europa.eu/newsroom/article29/items/612048>

²⁶ סעיף 38 (3) ל-GDPR.

²⁷ הנחיות Article 29 working party, לעיל ה"ש 25, בעמ' 15.

²⁸ שם.

²⁹ פסי' 7-10 לפסק הדין של בית הדין האירופי לצדק, *Leistriz v. LH*, EUECJ C-534/20 (22 June 2022), <https://www.bailii.org/cgi-bin/format.cgi?doc=/eu/cases/EUECJ/2022/C53420.html>

³⁰ Thomas Albermann, *Update: Scope of protection against dismissal and removal of the data protection officer - incompatibility with chairpersonship of the works council*, BIRD & BIRD (Oct. 27, 2023), <https://tinyurl.com/2p9u494c>

³¹ פסי' 35 לפסק הדין *Leistriz Case C-534/20*, לעיל ה"ש 29.

³² סעיף 38 (5) ל-GDPR.

³³ סעיף 38 (6) ל-GDPR.

במקביל בתפקיד שקשור לעיבוד המידע בארגון או לקביעת מטרות של עיבוד המידע,³⁴ או בתפקיד ניהולי בכיר.³⁵

אחריות

ה-DPO אינו אחראי אישית במקרה של אי-ציות ל-GDPR. כאמור, האחראים הם בעל השליטה במידע ומעבד המידע.³⁶ לפי פרשנות הגוף המייעץ ניתן לפרש את הפטור מאחריות אישית ככזה שמתקשר רק לאחריות אישית מול הרשות המאסדרת, כך שאינו שולל חבות אישית של DPO חיצוני בהתאם לחוזה שלו עם החברה ודיני הנוזיקין הכלליים, או של ה-DPO כעובד של החברה כלפי החברה שבה הוא מועסק.³⁷

תמיכה מהארגון בתפקיד ה-DPO

ב-GDPR מוגדר כי בעל השליטה במידע ומעבד המידע אחראים לוודא שה-DPO יוכל למלא את תפקידו בצורה הראויה ביותר ובזמן.³⁸ זאת על ידי הקצאת משאבים תשתיות וצוות במידת הצורך למילוי משימותיו, גישה למידע ולתהליכי העיבוד, ואף לאפשר ל-DPO לשמור על רמת מומחיותו למשל על ידי יציאה להכשרות כדי שיהיה מעודכן בהתפתחויות בתחום.³⁹

2. מסקנות לגבי יישום התפקיד באיחוד האירופי / תוצאות בשטח

כניסת תפקיד ה-DPO לפרקטיקה לא התבצעה בצורה חלקה. מאז שמינוי DPO הפך לדרישה מחייבת ברגולציה מ-2001 וביתר שאת לאחר התקנת ה-GDPR התעוררו בשטח קשיים בהטמעת התפקיד בארגונים, הבנת מיקומו בחברה וכיצד יש לעבוד איתו בשיתוף פעולה. להלן נתייחס לקשיים העיקריים שהתעוררו בהטמעת התפקיד בשטח.

חוסר מודעות לחובת המינוי

בבדיקה שערך ב-2023, הממונה האירופי על הגנת המידע (EDPS) (להלן: "הממונה") זיהה כי גופים מסוימים, בכללם גופים ציבוריים, לא מינו DPO למרות שהיו מחויבים בכך ב-GDPR.⁴⁰ לרוב הדבר לא נעשה במכוון וביודעין, אלא מחוסר מודעות לכך שפעילות הארגון מחייבת מינוי DPO לפי תקנה 37(1) ל-GDPR.⁴¹ העלאת המודעות לחובת מינוי DPO בארגון היא הכרחית לצורך הבטחת ציות בפועל.

³⁴ פסי' 38-46 לפסק הדין של בית הדין האירופי לצדק, X-FAB Dresden GmbH & Co. KG, EUECJ C-453/21 (09 February 2023), <https://www.bailii.org/cgi-bin/format.cgi?doc=/eu/cases/EUECJ/2023/C45321.html>, (2023).

³⁵ הנחיות Article 29 working party, לעיל ה"ש 25, בעמ' 16.

³⁶ שם, בעמ' 17.

³⁷ Lee Matheson, *DPO liability and potential insurance coverage*, IAPP, <https://iapp.org/news/a/dpo-liability-and-potential-insurance-coverage/>.

³⁸ סעיף 38 ל-GDPR.

³⁹ הנחיות Article 29 working party, לעיל ה"ש 25, בעמ' 14.

⁴⁰ European Data Protection Board, *Designation and Position of Data Protection Officers* (16 January 2024), 14-15, נמצא ב: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.

⁴¹ סעיף 37(1) ל-GDPR.

היעדר משאבים מספקים

בעמדת הממונה משנת 2005, לאחר כניסת הרגולציה מ-2001 לתוקף, עלה הקושי במינוי DPO במשרה מלאה, שכן לעסקים מסוימים אין יכולת כלכלית לכך.⁴² גם לאחר כניסת ה-GDPR לתוקף מצא הממונה בבדיקתו האחרונה כי לדעת 61% מה-DPOs במגזר הציבורי ו-33% מה-DPOs בחברות הפרטיות שסקר ברחבי האיחוד, אין להם משאבים מספקים ליישום חובותיהם. במגזר הציבורי היה גם משמעותית פחות נפוץ של-DPO יהיו חברי צוות או סגן, שיהיה לו תקציב עצמאי ושתהיה לו שליטה על התקציב שלו.⁴³ נראה כי גופים במגזר הציבורי נטו להיות מודעים פחות לחשיבות התפקיד, או שחסרו להם התמריצים המתאימים למינוי וקידום התפקיד בארגון.

ניגוד עניינים והיעדר עצמאות

הממונה מצא שבחברות רבות, כנראה לשם חיסכון בעלויות, ה-DPO משמש בנוסף כבעל תפקיד אחר בארגון, ועוסק בפועל בתפקידיו כ-DPO חלק מועט מהזמן.⁴⁴ בסקר שערך בשנת 2024, הממונה מצא כי במוצע, פחות ממחצית מה-DPOs שנסקרו עבדו במשרה מלאה. מתוך אלה שעבדו בחלקיות משרה ועסקו בעבודות אחרות במקביל – ארגונים רבים ציינו שהם מועסקים כחברי הנהלה בארגון או עוסקים ישירות בעיבוד מידע בארגון, בניגוד להנחיות ה-GDPR ובאופן שמעמיד אותם בניגוד עניינים מובהק.⁴⁵ סוגיות אלה מצביעות על פערי אכיפה של הרשויות באירופה.⁴⁶

בנוסף לכך, בארגונים גדולים, הממונה זיהה נטייה של חברות למנות מספר עובדים לסיוע ל-DPO. במקרים מסוימים, מונו סגנים ל-DPO, שמילאו את תפקידו בעת היעדרותו. הממונה, עוד בשנת 2005, המליץ לקבוע שהמנגנונים בחקיקה שמבטיחים את עצמאותו של ה-DPO יחולו גם על כל מי שממלא את תפקידו בפועל.⁴⁷ ב-GDPR אין התייחסות לכך, ויכולה להיות לכך משמעות גם בהיבט של דרישת היעדר ניגוד עניינים בעת ביצוע התפקיד. הדוח משנת 2023 הכיר בכך שיייתכן שבארגונים מסוימים יהיה צורך ממשי בצוות כזה על מנת למלא את תפקידי ה-DPO ברמה מספקת.⁴⁸ ה-GDPR גם מאפשר מינוי של DPO משותף לכמה חברות קשורות, בתנאי שיהיה נגיש בקלות לכולן.⁴⁹ ניתן למנות DPO משותף גם על ידי מיקור חוץ, אולם הממונה זיהה כי לעיתים ארגונים שמספקים שירותי DPO לחברות משרתים מספר לקוחות גדול מאוד, באופן שמעלה חשש לכך שלא יבצעו את תפקיד ה-DPO כראוי.⁵⁰

European Data Protection Supervisor, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (2005), p.7, https://www.edps.europa.eu/sites/default/files/publication/05-11-28_dpo_paper_en.pdf

[Designation and Position of Data Protection Officers](#), לעיל ה"ש 40, בעמ' 16.⁴³

Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, לעיל ה"ש 42, בעמ' 7.⁴⁴

Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 24-25.⁴⁵

שם, בעמ' 25.⁴⁶

Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, לעיל ה"ש 42, בעמ' 9.⁴⁷

Article 29 working party, לעיל ה"ש 25, בעמ' 14.⁴⁸

Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, לעיל ה"ש 42, בעמ' 8; סעיף 37 (2) ל-GDPR.⁴⁹

Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 15.⁵⁰

תפיסת תפקיד ה-DPO בארגון

פער נוסף בין הוראות ה-GDPR ליישום בפועל שנמצא בסקר של הממונה האירופי נוגע למידת המעורבות של ה-DPO בהחלטות בארגון. כרבע מהמשיבים העידו שהם חשים כי לא מתייעצים איתם מספיק לגבי טיפול או פתרון בעיות הקשורות לעיבוד והגנה על נתונים אישיים, היוועצות הנדרשת כחלק מתפקידם וחובת מינוי ה-DPO בארגון. גם כאשר התייעצו עם המשיבים, כ-55% העידו כי לא מתחשבים בעצתם בפועל בקבלת ההחלטות בארגון. 26% מהמשיבים סירבו לענות על שאלה זו.⁵¹

במחקר שנערך בדנמרק, העידו DPOs כי ההנהלה מתייחסת לתפקידם כנגזרת של המחלקה המשפטית, שעליה למצוא את ה"אזורים האפורים" כדי לאפשר את המשך פעילות והתחדשות הארגון, ולא דווקא מתייחסת ל-DPO כמומחה ומתייחסת ברצינות לסיכונים והחששות שהוא מעלה במסגרת תפקידו.⁵² כאמור לעיל, ה-GDPR לא דווקא מכווין שה-DPO יהיה שותף בקבלת ההחלטות בארגון, אולם בפועל לשם עמידת הארגון בתקנות, מקבלי ההחלטות צריכים להישמע לעצתו בכל הנוגע לפרטיות ועיבוד מידע אישי. הציפייה היא שבמידה וארגון מדיר את ה-DPO ומתייחס אליו כחותמת גומי, עליו לדווח על כך לרשויות המפקחות.

היעדר כשירות מספקת

הממונה האירופי מצא פערים ברמת הידע והמומחיות בין המשיבים לסקר, החל ברמת הכשרתם והידע שלהם בכניסתם לתפקיד וכלה ברמת הכשרתם והידע הניתנים ל-DPO לשם מילוי תפקידו לאחר כניסתו לתפקיד. ה-GDPR קובע כי על ה-DPO להיות מומחה בתחום ולא רק בעל ניסיון,⁵³ רמת הידע והמומחיות הנדרשת מה-DPO משתנה בהתאם לאופי פעולות העיבוד המתבצעות בארגון.⁵⁴ עם זאת, כרבע מהמשיבים העידו כי מומחיות בתחום הגנת המידע וידע ברגולציה הנדרשת בפרט לא הייתה דרישה בעת מינום לתפקיד ה-DPO (הדבר מעלה פער גם בהיעדר הגדרת תפקיד מדויקת בעת איתור מועמד לתפקיד). בנוסף לכך, רוב המשיבים העידו כי הקצו להם 24 שעות או פחות במהלך השנה להכשרות מיועדות לתפקיד. בתחום מתפתח כמו זה, יש חשיבות לשמירה על ה"כושר" והתעדכנות ברגולציה והדינים הנדרשים.⁵⁵ עמימות ה-GDPR ביחס לרמת המומחיות והידע הנדרשים מקשה על הבנת הארגונים כיצד להטמיע את התפקיד כראוי בחברה, ואף עלולה להקשות על אכיפה מתאימה.

היעדר הגדרת תפקיד ומשימות ברורות

קושי נוסף בהטמעת תפקיד ה-DPO בארגונים נוגעת להגדרת תפקידו ומשימותיו. על אף התווית המשימות של ה-DPO בסעיף 39 ב-GDPR,⁵⁶ בסקר שביצע הממונה נמצא כי ארגונים רבים לא מגדירים בבירור את משימות ה-DPO ולא מבינים מה עליו לעשות בפרקטיקה בארגון. ישנם למשל DPOs שהעידו שהטילו עליהם משימות שמיועדות לביצוע הבקר.⁵⁷

⁵¹ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 24-22.

⁵² Nicholai Pfeiffer, The Difficult Role of the DPO, White Label Consultancy (10 March, 2020), <https://whitelabelconsultancy.com/2020/03/the-difficult-role-of-the-dpo/>

⁵³ סעיף 37(5) ל-GDPR.

⁵⁴ Recital 97 ל-GDPR.

⁵⁵ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 19-18.

⁵⁶ סעיף 39 ל-GDPR.

⁵⁷ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 22-19.

3. הדין המצוי בישראל

אין בישראל חובה כללית למנות DPO, אך קיימות חובות פרטניות למינוי DPO בהקשרים ספציפיים, כולם ציבוריים. לדוגמה, חוק נתוני אשראי,⁵⁸ קובע כי נגיד בנק ישראל ימנה ממונה על הגנת הפרטיות, אשר יהיה עובד בנק ישראל;⁵⁹ חוק הכללת אמצעי זיהוי ביומטריים,⁶⁰ קובע כי שר הפנים, בהסכמת שר המשפטים, ימנה ממונה על הגנת הפרטיות במאגר מבין עובדי רשות האוכלוסין, הגם שלא קיימת חובה כללית בדין.⁶¹

על רקע היעדר חובה בדין, הרשות להגנת הפרטיות ממליצה על מינויו של DPO באופן וולונטרי.⁶² הרשות ממליצה שממלא התפקיד יהיה בעל הכשרה וידיעה מתאימים בתחום הפרטיות, יהיה עצמאי בתחום פעילותו, יהיה מעורב בכל הנושאים המהותיים הנוגעים למידע אישי בארגון, יבקר ויפקח על קיום הוראות ההגנה על הפרטיות מכוח החוק והתקנות, וכן יבצע תסקיר השפעה על הפרטיות להחלטות בארגון ויקבע את הנהלים והמדיניות בארגון בכל הנוגע לפרטיות.⁶³

בין ממונה הגנת פרטיות לממונה אבטחת מידע

סעיף 17 לחוק הגנת הפרטיות, התשמ"א-1981 מחיל חובת מינוי של ממונה על אבטחת מידע בגופים ציבוריים, בחברות עם מעל חמישה מאגרי מידע, בבנקים, בחברות ביטוח ובחברות דירוג או הערכת אשראי. הממונה על אבטחת המידע יהיה אחראי על תכנית לבקרה שוטפת של עמידה בתנאי אבטחת המידע בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 וכן עמידה בדרישות התקנות, בהתאם לרמת האבטחה של המאגר.⁶⁴ הממונה נדרש להכין נוהל אבטחה למאגר המידע, וכן להכין ולבצע תוכנית לבקרה שוטפת על ביצוע ההוראות מכוח תקנות אבטחת המידע.⁶⁵ הוראות אלה כוללות, בין היתר, ניהול הרשאות הגישה למאגר, תיעוד הגישה למאגר ותיעוד אירועי אבטחה. לממונה על אבטחת המידע יש אחריות אישית לאבטחת המידע במאגרים, בנוסף לאחריות שחלה על בעלי ומנהלי מאגר המידע.⁶⁶

יש קשר ברור בין אבטחת מידע במאגר לבין הבטחת פרטיות המידע בארגון – כאשר מידע אינו מאובטח, עולה החשש לכך שאינו פרטי. מידע שאילו ניגשים עובדים שאינם רשאים לכך, או גורמים חיצוניים לארגון מבלי שקיבלו לאישור לכך, הוא מידע שעשוי להיעשות בו שימוש שלא למטרות שלשמן הוא נועד. יש אף חשש שמידע כזה יזלוג אל מחוץ לארגון, ומחוץ לטווח הבקרה שלו. אין ספק שזליגת מידע שכזו היא פגיעה בסודיות המידע השמור במאגר ובפרטיות האנשים ששמור מידע לגביהם במאגר, כשם שהיא פגיעה באבטחתו של המאגר. על כן, יש דמיון בין תחומי האחריות האפשריים של הממונה על אבטחת המידע ושל ה-DPO. אולם ניתן להבחין במספר נקודות שוני עיקריות ביניהם:

⁵⁸ חוק נתוני אשראי, התשע"ו-2016.

⁵⁹ סעיף 18 לחוק נתוני אשראי.

⁶⁰ סעיף 26 לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי במסמכי זיהוי ובמאגר מידע, התשע"ט-2009.

⁶¹ הרשות להגנת הפרטיות "מינוי ממונה הגנה על הפרטיות בארגונים, תפקידיו ותחומי אחריותו" (פרסום מקצועי) **משד המשפטים** (25.01.2022). https://www.gov.il/he/pages/dpo_doc_kit

⁶² שם.

⁶³ שם.

⁶⁴ התקנות מגדירות ארבע רמות של אבטחת מידע - רמת אבטחה למאגר מידע המנוהל על-ידי יחיד, רמת אבטחה בסיסית, רמת אבטחה בינונית ורמת אבטחה גבוהה, שהסיווג לגביהן נעשה על פי קריטריונים של גודל מאגר המידע, מספר המורשים אליו, סוג המידע ורגישותו. ראו התוספת הראשונה והשנייה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

⁶⁵ סעיף 3 לתקנות הגנת הפרטיות (אבטחת מידע).

⁶⁶ סעיף 17 ו-17ב(ב) לחוק הגנת הפרטיות, התשמ"א-1981.

DPO	ממונה על אבטחת מידע	
כלל היבטי הפרטיות ועיבוד המידע בארגון	אבטחת מאגר המידע	היקף האחריות
פרטיות המידע והיבטי פרטיות בעבודת הארגון	אבטחת המידע	תכלית מרכזית
משפטי/בקיאות בדיני הגנת הפרטיות	טכני	עיקר הידע הנדרש

בעוד שאת ה-DPO יוכלו להנחות עקרונות של חוק הגנת הפרטיות כגון קבלת הסכמה לשיתוף מידע, ויהיה אחראי על מדיניות הפרטיות בארגון, שיתוף מידע עם צדדים שלישיים, ובגוף ציבורי גם קבלת אישור לשיתוף מידע בין גופים ציבוריים, הממונה על אבטחת המידע אחראי אך ורק לוודא שהמידע במאגר המידע עליו הוא אחראי שמור – הן מפני חדירות עוינות מבחוץ והן מפני דליפות מבפנים, בין בזדון ובין ברשלנות. אחריות זו תחומה וממוקדת בהרבה מאחריותו של ה-DPO, שאחראי על כלל עיבוד המידע בארגון, בהתאם לסטנדרטים של חוק הגנת הפרטיות.

בטיט הנחיית רשות הגנת הפרטיות בנושא אבטחת מידע, הרשות מציעה כי בחברות שעיבוד מידע אישי מצוי בליבת הפעילות שלהן או שפעילותן יוצרת סיכון מוגבר לפרטיות, האחריות על ביצוען של דרישות פיקוחיות בעיקרן כדוגמת אישור עקרונות מרכזיים בנוהל אבטחת מידע ארגוני, קיום דיונים על סקרי סיכונים ובחינת ביקורות תקופתיות בנוגע לעמידה בארגון צריכה להיות של הדירקטוריון.⁶⁷ הרשות מנמקת את עמדתה בכך שהדירקטוריון הוא הגורם המתאים והיעיל בקבלת החלטות שקשורות בנושאים מהותיים יותר.⁶⁸

הדירקטוריון רשאי גם להטיל אחריות על גורם אחר בחברה. מכך שהרשות ותקנות אבטחת המידע לא מטילות ישירות אחריות על הנושאים המהותיים על ממונה אבטחת המידע, ניכר כי תפקיד ממונה אבטחת המידע הוא תפקיד טכני בעיקרו.

4. ישראל: המלצות חקיקה

בפרק זה נאגד את כל ההיבטים שיש לתת עליהם את הדעת בעת חשיבה על מסגרת חקיקתית מתאימה בנושא תפקיד ה-DPO בישראל. בסוף הפרק מרוכזות המלצותינו לפי נושאים.

מינוי DPO: חיוב או המלצה?

אפשרות אחת היא לקבוע בחוק חובה למנות ממונה הגנה על הפרטיות. בתקנה 37(1) ב-GDPR מפורטים המקרים בהם קיימת חובת מינוי, נזכיר: כשעיבוד המידע מתבצע על ידי רשות או גוף ציבורי (בהחרגת בתי משפט); כשפעולות הליבה של הארגון כוללות עיבוד מידע אישי ומתוקף טיבן, היקפן או מטרותיהן מחייבות ניטור שיטתי ומערכת של נושאי המידע בהיקף רחב; כשליבת עיסוק הארגון כוללת עיבוד מידע אישי רגיש בהיקף רחב.⁶⁹

⁶⁷ הרשות להגנת הפרטיות "הנחיה בנושא תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)" (פרסום מקצועי) **משרד המשפטים** 4 (25.01.2022), נמצא ב: https://www.gov.il/he/pages/2023privacy_protection_regulations

⁶⁸ שם.

⁶⁹ סעיף 37(1) ל-GDPR.

מדובר בהגדרה רחבה שבעקבותיה עולות שאלות פרשניות. הוועדה המקצועית של רשויות הפרטיות באיחוד האירופי פרסמה הנחיות ל-DPO ובהן התייחסה לשאלות הפרשניות הבאות: מה נחשב ל"רשות או גוף ציבורי"? מה נחשב ל"פעילויות ליבה" של ארגון? מהו "קנה מידה גדול" וכיצד ניתן לחשב אותו? ומהו "ניטור שיטתי ומערכתי"?⁷⁰

אם כן, במידה שרוצים לקבוע עקרונות כלליים לחובת מינוי DPO במקום כללים ברורים יש לבחון את ההשלכות. ייתכן שהקושי הפרשני ב-GDPR הוביל לחוסר המודעות שיש לארגונים באשר לחובה המוטלת עליהם למינוי DPO, כפי שנמצא בבדיקה שערך המפקח האירופי על הגנת המידע.⁷¹ ייתכן גם קושי באכיפת חובת המינוי או התדיינויות ארוכות אודות פרשנות חובת המינוי.

אפשרות אחרת מצויה בסעיף 23 בהצעת החוק של המכון הישראלי לדמוקרטיה (להלן: "הצעת המכון לדמוקרטיה").⁷² מוצע שם לקבוע חובת מינוי ממונה הגנה על הפרטיות כשמדובר בגוף ציבורי, בדומה לתקנה המקורית ב-GDPR.⁷³ בנוסף, מוצע שם לתחום מספרית את היקף החובה. ההצעה מפרידה בין ביצוע עיבוד מידע אישי (המחייב מינוי ממונה כשהמאגר כולל 200,000 נושאי מידע לפחות) לבין ביצוע עיבוד מידע רגיש (המחייב מינוי ממונה כשהמאגר כולל 100,000 נושאי מידע לפחות).⁷⁴ ההצעה מנמקת את תחמת היקף בכך שקביעת חובה כללית עלולה להטיל נטל לא סביר על גופים קטנים, ומנגד יש לשמור על כך שעיבוד מידע אישי ורגיש יפוקח על ידי ממונה בעל הגדרת פיקוח רחבה יותר מממונה על אבטחת מידע. תחומה מסוג זה יכולה לסייע בפתרון בעיות הפרשנות הקיימות מניסוח ה-GDPR.⁷⁵

עם זאת, ייתכנו מקרים בהם ארגונים יעבדו מידע רגיש מאוד אולם לא בהיקף רחב מספיק כפי שהוצע בהצעת המכון לדמוקרטיה, ואף בהיקף קטן מאוד. זאת כדוגמת עמותות וארגונים מהמגזר השלישי שעוסקים במידע רגיש מאוד, לרבות מידע סודי ומידע שבליבת צנעת הפרט, לעיתים קרובות של אוכלוסיות מוחלשות. למשל, סוכנויות אימוץ, עמותות שמתמקדות בסיוע במצבים רפואיים שונים, ועוד. יש לשקול האם נדרש ליחיד חובה או המלצה של מינוי על סמך קריטריונים שונים כשמדובר בארגונים מסוג זה, או שמא ליצור גוף המאפשר חובת היוועצות לאותם גורמים בהינתן המידע הרגיש שנמצא ברשותם. בהקשר זה יש להביא בחשבון מגבלות תקציביות של ארגונים מסוג זה, בפרט העובדה שהם לרוב מתקיימים מתרומות וללא כוונת רווח.

זאת ועוד, בדברי ההסבר להצעת המכון לדמוקרטיה יש התייחסות לאפשרות המנויה ב-GDPR למנות ממונה אחד למספר חברות בנות או על קבוצת גופים ציבוריים. הוצע שם להתייחס לכך בתקנות ולא במסגרת החוק. נוסף לכך שלטעמנו יש לשקול, במידה שמיעדים תקנות מסוג זה, גם את האפשרות למינוי ממונה הגנה על הפרטיות חיצוני לחברה ולא רק כהגדרת תפקיד פנימית, כמצוי ב-GDPR, וזאת בתנאי של היעדר ניגוד עניינים.⁷⁶

⁷⁰ הנחיות Article 29 working party, לעיל ה"ש 25, בעמ' 6-9.

⁷¹ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 14-15; ראו בנוסף דיון בנושא בפרק 2 למסמך זה תחת הכותרת " חוסר מודעות לחובת המינוי".

⁷² רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר הצעת חוק הגנת הפרטיות התשע"ט-2019 המכון הישראלי לדמוקרטיה (2019).

⁷³ שם, בסעיף 23(א)(1).

⁷⁴ שם, בסעיף 23(א)(2) ו-23(א)(3).

⁷⁵ שם, בעמ' 107.

⁷⁶ סעיף 37(6) ל-GDPR.

לעומת זאת, ישנה אפשרות להותיר את מינוי ה-DPO כהחלטה וולונטרית, ולעודד ארגונים לעשות כן בדרכים שונות. לפי הרשות להגנת הפרטיות, גם בהיעדר חובה חוקית, ראוי ומומלץ שארגונים שאוספים ומעבדים מידע אישי ימנו באופן וולונטרי ממונה הגנת פרטיות. זאת כדי לסייע לארגון לעמוד בהוראות הדין, לאותת כלפי חוץ שהארגון עושה את מירב המאמצים לצמצום סיכון לפגיעה במידע אישי, ולאפשר שיתוף פעולה מיטבי עם הרשות.⁷⁷

ניתן אף לנקוט גישת ביניים, כפי שנוקטת שוויץ, אשר רמת ההגנה על המידע בתחומה, בדומה לישראל נחשבת ל"נאותה" (adequate) ל-GDPR.⁷⁸ בשוויץ מפרידים בין חברות פרטיות לגופים פדרליים: המועצה הפדרלית מחויבת להסדיר מינוי של DPO בגופים פדרליים,⁷⁹ ואילו חברות פרטיות יכולות למנות DPO באופן וולונטרי ("Private controllers may appoint a data protection officer").⁸⁰ לאחר המינוי (בין אם מכוח חובה או וולונטרי) יחולו על ה-DPO אותן הדרישות.

עם זאת, בארגנטינה לא הייתה עד כה חובת מינוי DPO ואילו בהצעה לתיקון החוק שהוגשה בספטמבר 2023 יש התייחסות להוספת חובת מינוי DPO.⁸¹ ארגנטינה גם עברה את בחינת ה"תאימות" ל-GDPR לאחרונה, ושם התייחסו במפורש להצעת חוק זו.⁸² ייתכן, אם כן, שזהו סממן לכך שצריכה להיות התייחסות בחוק למינוי DPO כדי להיוותר במעמד ה-adequacy.

הגדרת תפקיד

בהתאם למסקנות שעלו מיישום ה-GDPR באיחוד האירופי, נראה כי יש אי-בהירות רבה באשר לתפקיד ה-DPO בארגון, וייתכן שהדבר נובע מהכלליות של הגדרת התפקיד ב-GDPR.⁸³ כתוצאה מהיעדר הבהירות לגבי אופי התפקיד, החשיבות של התפקיד בארגון פוחתת וכך גם כוחו להשפיע על קבלת החלטות. עם זאת, הגדרות ספציפיות מדיי עלולות להקשות על התאמה של תפקיד ה-DPO לתפקוד הארגונים, מאחר ומאפייניו של כל ארגון שונים.

בהצעת המכון לדמוקרטיה הוצעה מסגרת כללית לתפקידי הממונה על הגנת הפרטיות. ישנה התייחסות להבטחת קיום הוראות החוק ואחריות לטיפול בפניות הציבור ובפניות הרשות.⁸⁴ בשוויץ מוגדרות שתי משימות, כלליות גם כן: מתן הכשרה וייעוץ לבקר המידע בנושא הגנת המידע, ומתן תמיכה ביישום תקנות הגנת המידע.⁸⁵

⁷⁷ הרשות להגנת הפרטיות "מינוי ממונה הגנה על הפרטיות בארגונים, תפקידי ותחומי אחריותו" (2022), לעיל ה"ש 61.

⁷⁸ סעיף 45 ל-GDPR מאפשר למוסדות האיחוד האירופי להגדיר מדינות מחוץ לאיחוד האירופי שרמת הגנת המידע שלהן הולמת את דרישות ה-GDPR. הגדרת מדינות ככאלה מאפשרת את זרימת המידע למדינות אלה מהאיחוד האירופי ללא נקיטה של אמצעים נוספים להגנתו. ראו -international-dimension-of-data-protection/adequacy-decisions_en

⁷⁹ סעיף 10(4) ל-235.1 Federal Act of 25 September 2020 on Data Protection (Data Protection Act, FADP).

⁸⁰ סעיף 10(1) לחוק השוויצרי, לעיל ה"ש 79.

⁸¹ Florencia Rosati, *Argentina: New data protection bill - what you need to know*, Data Guidance (June 2023), <https://www.dataguidance.com/opinion/argentina-new-data-protection-bill-what-you-need>

⁸² European Commission, *Report From The Commission To The European Parliament And The Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC* p.8 (15.01.2024), https://commission.europa.eu/document/download/f62d70a4-39e3-4372-9d49-e59dc0fda3df_en?filename=JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf

⁸³ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 19-22.

⁸⁴ הצעת החוק של המכון הישראלי לדמוקרטיה (2019), לעיל ה"ש 72, בעמ' 106.

⁸⁵ סעיף 10(2) לחוק השוויצרי, לעיל ה"ש 79.

בהתחשב בבעיות שעלו ביישום ה-GDPR באיחוד האירופי בעקבות התוויה כללית של תפקידי ה-DPO, יש לדעתנו צורך בפירוט רב יותר על תפקידיו של ה-DPO בהיבטים יומיומיים של תפקודו. בשל האופי הכללי של חקיקה ראשית, לעמדתנו יש לתעדף פירוט של תפקידים אלה בתקנות.

הרשות להגנת הפרטיות בעמדתה לגבי מינוי ממונה הגנה על הפרטיות מפרטת את התפקידים והמשימות שמומלץ לשקול להטיל על הממונה בשלושה תחומים: הסדרת תהליכי ניהול מידע, פיקוח ובקרה והדרכה והטמעה. ניתן לשאוב השראה מתתי-המשימות המוגדרות שם.⁸⁶

בהמשך לכך, אנו מציעים שעל הממונה להגנת הפרטיות תוטל בחקיקה החובה לוודא את קיום הוראות חוק הגנת הפרטיות על-ידי בעלים או מנהל של מאגר מידע, וכן שתפקידו יהיה להגביר את המודעות לחשיבות הפרטיות והשלכותיה בארגון.

בנוסף, בהשראת ה-GDPR,⁸⁷ הצעת המכון לדמוקרטיה,⁸⁸ וההנחיות בקנדה⁸⁹ יש לדעתנו לראות ב-DPO כאיש קשר בנושא הפרטיות בארגון – הן כאיש קשר עבור הרשות להגנת הפרטיות והן כאיש קשר לנושאי המידע. אין חובה לקבוע את אופן יצירת הקשר בחקיקה, וניתן לקבוע אמצעי יצירת קשר אפקטיביים בתקנות.

ממונה על הגנת הפרטיות וממונה על אבטחת מידע – יחסי גומלין

בדין הישראלי קיים כבר, כידוע, תפקיד ממונה אבטחת מידע, המעוגן בחוק ובתקנות הגנת הפרטיות (אבטחת מידע) מ-2017. אין ספק שקיים קשר בין אבטחת המידע בארגון להגנה על הזכות לפרטיות,⁹⁰ אך עולה השאלה האם נכון שתפקיד ממונה על הגנת הפרטיות יכיל בתוכו גם את האחריות על אבטחת המידע בארגון, קרי, איחוד שני התפקידים לכדי תפקיד אחד. לאיחוד תפקידים יש יתרון מבחינת הקצאת המשאבים הנדרשת לאותו בעל תפקיד במקום להוסיף דרישה לארגונים לגייס משאבים נוספים, וכן מניעת מצבים של ביצוע פעולות חופפות על ידי שני בעלי תפקידים. יוזכר כי מהסקר של הממונה האירופי עלה כי מינוי DPO במשרה מלאה מקשה על עסקים שאין להם יכולת כלכלית לספק את המשאבים הדרושים לבעל התפקיד, כנדרש בחוק.⁹¹

עם זאת, אנו סבורים שהחסרונות שבאיחוד התפקידים עולים באופן מובהק על היתרונות. המדובר בתפקידים שונים במהותם, שהדגשים שבהם שונים, ודורשים כישורים וצורת חשיבה שונים. כך, בעוד שרצוי שממונה על אבטחת המידע יהיה אדם בעל ידע טכני, ממונה על הגנת הפרטיות לא נדרש לכך, לפחות לא במסגרת ביצוע ליבת תפקידיו. כמו כן, איחוד התפקידים עלול לגרור ירידה ברמתם של הממונים על אבטחת המידע בארגונים, שכן כעת אבטחת מידע לא תהיה ליבת התפקיד שלהם, אלא חלק מתפקיד כולל.

⁸⁶ הרשות להגנת הפרטיות "מינוי ממונה הגנה על הפרטיות בארגונים, תפקידיו ותחומי אחריותו" (2022), לעיל ה"ש 61, בעמ' 5-4.

⁸⁷ סעיפים (d)(1)39, (e)(1)39 ו-(4)38 ל-GDPR.

⁸⁸ הצעת החוק של המכון הישראלי לדמוקרטיה (2019), לעיל ה"ש 72, בעמ' 107.

⁸⁹ על פי מסמך העקרונות של נציב הפרטיות הקנדי בנוגע ליישום החוק הקנדי להגנה על מידע אישי ומסמכים אלקטרוניים (The Office of the Privacy Commissioner of Canada, PIPEDA Self-Assessment Tool, Principle 8 (Openness) (August 13, 2001), https://www.priv.gc.ca/media/1196/pipeda_sa_tool_200807_e.pdf

⁹⁰ הצעת החוק של המכון הישראלי לדמוקרטיה (2019), לעיל ה"ש 72, בעמ' 106-109.

⁹¹ ראו דיון בנושא בפרק 2 למסמך זה תחת "היעדר משאבים מספקים", וגם Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, לעיל ה"ש 42, בעמ' 7; Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 16.

לבסוף, יש להותיר גמישות ולאפשר מקרים בהם תהיה חובת מינוי ממונה אבטחת מידע אך לא ממונה על הגנת פרטיות, ולהיפך.

הגדרת ידע ומומחיות

ה-GDPR מציין כי יש למנות DPO על בסיס תכונות מקצועיות שלו, ובייחוד מומחיות בדיני הגנת המידע ושיטות העבודה שיסייעו בעמידה במשימותיו.⁹² אותה רמת מומחיות לפי ה-GDPR היא אינדיבידואלית לכל ארגון, בהתבסס על הליכי העיבוד וההגנה הנדרשים על הנתונים המסוימים בחברה.⁹³ מדובר שוב בהגדרת סטנדרט עמום אולם ייתכן שזו האפשרות המיטבית לאור רמות רגישות מגוונות של מידע, והבדלים במורכבות וכמות נתונים שונים ביחס לכל ארגון.⁹⁴

עם זאת, העמימות הזו מובילה לכך שישנם ממוני הגנת פרטיות שאינם בעלי ההכשרה והידע הנדרשים לשם מילוי תפקידם, והממונה באיחוד האירופי אף מצא שישנם ארגונים שכלל לא דורשים רמת מיומנות מסוימת. בנוסף לכך, הממונה מצא כי בעלי התפקיד לא מקבלים הכשרות גם לאחר כניסתם לתפקיד, לשם התעדכנות בתחום המתפתח.⁹⁵ על כן, יש לחשוב האם צריכים לייצר כללים יותר ברורים ביחס לדרישת הכשרת הממונה על הגנת הפרטיות, למשל במסגרת תקנות, או שמא יש להשאיר את הסטנדרט העמום.

בקנדה שגם היא "תואמת" ל-GDPR, כחלק ממדריך שהוציא משרד נציב הפרטיות של קנדה (OPC), נאמר שכשירות למילוי תפקיד ה-privacy officer נחשבת ליכולת להפגין ידע על המדיניות והנהלים לטיפול במידע אישי של הארגון, וגם ידע על אחריות הארגון במסגרת ה-PIPEDA (חוק הגנת המידע הקנדי). כלומר הכשירות נסמכת על צרכי הארגון בנוסף לידעת החוק. בנוסף בקנדה יש הנחיה שעל ה-DPO להיות מסוגל לנהל או לפקח על חקירת תלונות.⁹⁶

בהצעת המכון לדמוקרטיה הוצע ששר המשפטים יקבע בתקנות את תנאי הכשירות הנדרשים, וזאת מתפיסה דומה לזו ב-GDPR שהכשירות הנדרשת משתנה מארגון לארגון.⁹⁷

במידה שייקבעו תנאים בתקנות נמליץ לשלב גם עקרונות כלליים המאפשרים גמישות בהתאמת התפקיד לארגון וזאת משום שמחד גיסא, הגדרת כשירות מסוימת מדיי עלולה לצמצם את טווח המועמדים הפוטנציאליים למינוי לתפקיד, אך מאידך גיסא, הדיוק בדרישות הכשירות לתפקיד יכולות ליחד אותו מתפקיד ממונה על אבטחת המידע, ולייצר תפקיד מהותי.

בנייר העמדה שלה, הרשות להגנת הפרטיות התייחסה לכך שלממונה צריכה להיות הבנה מיטבית של תהליכים בארגון ברמה טכנולוגית ועסקית ובנוסף לכך גם לבחון התאמת התהליכים לדרישות החוק ולמדיניות הארגון. הרשות מציעה תנאי סף מוגדר - הכשרה אקדמית בתחום מסוים (משפטים, חשבונאות, טכנולוגיית מידע וכו'); וגם תנאי סף רחבים יותר - ידיעה מעמיקה של הדינים בישראל והיכרות עם הדינים באירופה ובארה"ב, הבנה נאותה בתחום טכנולוגיות המידע בכלל ובתחום אבטחת המידע בפרט וכן אתיקה

⁹² סעיף 37(5) ל-GDPR.

⁹³ Recital 97 ל-GDPR.

⁹⁴ הנחיות Article 29 working party, לעיל ה"ש 25, בעמ' 12.

⁹⁵ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 18-19.

⁹⁶ PIPEDA Self-Assessment Tool, לעיל ה"ש 90, תחת Principle 10 – Challenging Compliance בעמ' 33-34.

⁹⁷ הצעת החוק של המכון הישראלי לדמוקרטיה (2019), לעיל ה"ש 72, בעמ' 106-107.

מקצועית. בנוסף הרשות מתייחסת לכשירות הנדרשת ביחס לארגון עצמו, בדומה לקנדה, וטוענת שעל הממונה להכיר את הפן העסקי של ניהול הארגון.

כיום יש בישראל קורסים אחדים להכשרת ממוני הגנת הפרטיות.⁹⁸ ברובם מוצעים תכנים מקצועיים של סקירת הדינים וכלים פרקטיים לעבודת ממונה הגנת פרטיות בארגון כדוגמת בניית סקר סיכונים, התמודדות עם ביקורות, מתן מענה למחלקות וכו'. ניתן לשקול אפשרות לחייב השתתפות בקורס כשירות שכזה וחיוב ביצוע קורסי כשירות תקופתיים, על מנת לשמור על רמת כשירות ומומחיות אחידה בין ארגונים. עם זאת, ייתכן שהדבר יטיל נטל כבד מדי על גופים, למשל במגזר השלישי, שנעדרים המשאבים המספקים לממן יציאה להכשרות מסוג זה. ניתן להציע קורסי כשירות מטעם הרשות שיהיו זמינים בחינם או במחיר מסובסד/מפוקח, אולם גם כאן נכנסים שיקולי תקציב (הפעם מצד המדינה) שיש לתת עליהם את הדעת.

עצמאות וניגוד עניינים

כפי שקבוע ב-GDPR, תפקידו של ה-DPO מחייב עצמאות ופעולה בהיעדר ניגוד עניינים.⁹⁹ עצמאות והיעדר ניגוד עניינים יאפשרו ל-DPO למלא את תכלית תפקידו – הגנה על פרטיות נושאי המידע שהארגון מאחסן או מעבד את המידע שלהם. פגיעה בעצמאותו או פעולה בניגוד עניינים תעלה חשש לכך שיעדיף את האינטרס הכלכלי של הארגון על פני המחויבויות של הארגון מכוח החוק ועל פני הגנה על הפרטיות.

במסגרת ה-GDPR לא נקבעה מסגרת מחייבת של תפקידים בארגון שבהם DPO לא יוכל להחזיק,¹⁰⁰ וכאמור לעיל האיחוד האירופי מצא בסקריו ש-DPOs רבים כיהנו במקביל גם כחברי הנהלה בארגונים שבהם הם עובדים.¹⁰¹ כהונה במקביל כחבר הנהלה מעלה חשש כבד לכך שה-DPO יעדיף את טובתו הכלכלית של הארגון על פני מחויבויות הארגון להגנת הפרטיות של לקוחותיו, ושיתפוס את תפקידו כ-DPO כתפקיד משני שמטרתו לאפשר את הפגיעה בפרטיות בצורה שמיטיבה עם הארגון.

מכך ניתן להסיק שהמסגרת החוקית שהוצבה ב-GDPR כללית מדי, ויש להגדיר במפורש בחקיקה או בתקנות אילו בעלי תפקידים אינם יכולים לכהן במקביל כ-DPOs, כרשימה פתוחה. דוגמאות ברורות לכך הן מנכ"ל, סמנכ"לים וחברי דירקטוריון.¹⁰² הותרת הרשימה פתוחה תאפשר שיקול דעת לקביעה מתי לא ראוי שממונה הגנה על הפרטיות במידע ישמש גם כבעל תפקיד אחר בארגון, על בסיס מאפייני הארגון, התפקיד, והקשר שלו לעיבוד המידע.

עצמאות ה-DPO יכולה לבוא לידי ביטוי הן במילוי תפקידו והן בהגנה מפני פיטורין. בהקשר זה, ייתכנו מקרים בהם עצמאות רבה מדי תפגע בהגנה על המידע בארגון, לדוגמה כאשר ה-DPO אינו כשיר למלא את תפקידו, פועל בניגוד עניינים או הואשם בעבירות שנוגעות לאבטחת מידע.¹⁰³ כמו כן, הגבלת פיטורין עשויה לגרום לארגונים להעדיף העסקת DPO חיצוני בחוזה קצוב,¹⁰⁴ כך שניתן יהיה להפסיק את ההתקשרות

⁹⁸ כדוגמת: קורס שמציעה אוניברסיטת תל-אביב, https://law.tau.ac.il/HP-Legal_Art/1234; קורס שמציעה המכללה העסקית <https://www.cbc.org.il/course.aspx?id=61823>; קורס שמציעה לשכת עורכי הדין <https://www.ibar.org.il/shop/60-prtyvt-qvrs-mmvnh-hgnt-hprtyvt-dpo-pbrvar-2024-338>

⁹⁹ סעיף 38(3) ל-GDPR מבטא 3 היבטים של עצמאותו של ה-DPO: (1) הוא לא יקבל הנחיות ביחס לעבודתו; (2) הוא לא יפוטרו או ייפגע בשל ביצוע תפקידו; (3) הוא ידווח לדרג הניהולי הגבוה ביותר.

¹⁰⁰ סעיף 38(6) ל-GDPR מצייין שה-DPO יוכל לבצע תפקידים אחרים, אך יש לוודא שביצוע תפקידים אלה לא יוביל לניגוד עניינים.

¹⁰¹ Designation and Position of Data Protection Officers, לעיל ה"ש 40, בעמ' 24-26.

¹⁰² הנחיות working party Article 29, לעיל ה"ש 25, בעמ' 16.

¹⁰³ פסי' 32-34 לפסק הדין X-FAB Dresden C-453/21, לעיל ה"ש 34.

¹⁰⁴ Albermann, לעיל ה"ש 30.

בקלות. לעמדתנו, החסרונות עולים על היתרונות בהקשר זה, בוודאי במדינה קטנה כישראל, שבה סביר מאוד שארגונים שמספקים שירותי ממונה הגנה על הפרטיות חיצוניים ייעצו במקביל לחברות מתחרות, באופן שיציב את הארגון עצמו בניגוד עניינים. על כן, יש להימנע מקביעת הגנות רחבות בחקיקה מפני פיטורי הממונה, וכך לעודד מינוי ממונה פנימי. בנוסף, ניתן לאמץ את הכלל הקבוע ב-GDPR, לפיו אין להנחות את ה-DPO ביחס לפעילותו, ואין לפטר אותו או לפגוע בתנאי העסקתו בשל ביצוע תפקידיו.¹⁰⁵

אחריות

ה-GDPR לא מתייחס מפורשות לסוגיית אחריות ה-DPO. בהנחיות הוועדה המקצועית של רשויות הפרטיות באיחוד האירופי נאמר כי ל-DPO אין אחריות אישית במקרה של אי-ציות, אלא האחריות חלה על בעל השליטה במידע ומעבד המידע.¹⁰⁶ אף הצעת המכון לדמוקרטיה שותקת בעניין, אך בדברי ההסבר הכותבות מציינות את דיני החברות הקובעים אחריות על נושאי משרה בחברה ביחס לחובות הציות להוראות החוק והאחריות למילוי.¹⁰⁷

הרשות להגנה על הפרטיות פרסמה הנחיה בנושא "תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)". שם הרשות מטילה אחריות על הדירקטוריון על ביצוען של דרישות פיקוחיות בעיקרן של ממונה על אבטחת המידע. הנימוק לכך הוא שהדירקטוריון הוא הגורם המתאים והיעיל בקבלת החלטות שקשורות בנושאים מהותיים.¹⁰⁸ ניתן לשקול התייחסות שכזו אף כלפי חובות המוטלות על הממונה להגנה על הפרטיות בארגון. בנוסף, יש לשקול האם יש צורך בהפרדת האחריות בכל הנוגע לחובות מסוימות בין הממונה על הגנת הפרטיות, לבין בעל השליטה במידע ומעבד המידע, לבין הדירקטוריון או נושאי משרה אחרים.

במידה שמאפשרים לבצע מיקור חוץ לתפקיד ממונה הגנה על הפרטיות במידע, יש לשים לב שבהתאם לחוזה יהיה ניתן להטיל אחריות על הממונה החיצוני לפי דיני החוזים והנזיקין הכלליים.

שילוב תפקיד הממונה על הגנת הפרטיות בארגון

במענה לאתגר בתפיסת תפקיד ה-DPO בארגון שהוצג בפרק הקודם, יש לשקול האם צריך להגדיר בפועל תמיכה של הארגון בתפקיד הממונה, וכיצד. ה-GDPR והצעת המכון לדמוקרטיה שותקת בעניין זה.

בקנדה הנחיות ה-OPC מציינות במפורש שיש לתת לממונה תמיכה מההנהלה הבכירה וסמכות להתערב בנושאי פרטיות הנוגעים לפעולת הארגון. עמדה זו מתבטאת בהגדרת התפקיד, שם מתואר כי הממונה צריך להיות בעמדה של מקבל החלטות בכיר שנתמך בבירור בתפקידו על ידי ההנהלה הבכירה בקידום הפרטיות כערך תאגידי ובנוסף עליו להיות מסוגל להתערב בנושאי הפרטיות ברחבי הארגון בכל צורך.¹⁰⁹ הנחיות אלה מקנדה חופפות לעמדת הרשות ביחס למעמדו של ממונה הגנה על הפרטיות בארגון שטוענת כי מומלץ שהממונה יהיה חלק מההנהלה הבכירה של הארגון כדי שיוכל למלא באופן מיטבי את תפקידיו ומשימותיו. אמרה זו מצטרפת להנחיה לשמירה על היעדר ניגוד עניינים של הממונה עם תפקידיו השונים בארגון.¹¹⁰ ניתן

¹⁰⁵ סעיף 38(3) ל-GDPR.

¹⁰⁶ הנחיות Article 29 working party, לעיל ה"ש 25, בעמ' 17.

¹⁰⁷ הצעת החוק של המכון הישראלי לדמוקרטיה (2019), לעיל ה"ש 72, בעמ' 107.

¹⁰⁸ הנחית הרשות להגנת הפרטיות בנושא תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע), לעיל ה"ש 67, בעמ' 1.

¹⁰⁹ PIPEDA Self-Assessment Tool, לעיל ה"ש 91, תחת Principle 1 – Accountability בעמ' 6 – 10.

¹¹⁰ הרשות להגנת הפרטיות "מינוי ממונה הגנה על הפרטיות בארגונים, תפקידיו ותחומי אחריותו" (2022), לעיל ה"ש 61, בעמ' 1.

לשקול האם יש להוסיף כחלק מהגדרת התפקיד של הממונה, או כחלק מתנאי כשירותו מרכיב זה של ייחוס להנהלה הבכירה או לציין מפורשות כי על ההנהלה לשמוע לממונה.

אפשרות אחרת באמצעותה ניתן להבטיח כיבוד מעמד הממונה בארגון היא להתנות ביצוע פעולה או החלטה מסוימת בארגון שקשורה לעיבוד ושימוש מידע באישור של הממונה בארגון. בקנדה למשל, ה-OPC מנחה שבטרם הגדרת מטרה נוספת לשימוש במידע בארגון (כחלק מחובת עמידה בעיקרון "זיהוי המטרות" שנמצא בחוק בקנדה) הממונה צריך לקבוע אם היא ראויה, ולשקול כיצד ניתן להפחית סיכוני פרטיות פוטנציאליים.¹¹¹ ניתן לחשוב על מקבילות בדין או בהנחיות הישראליות שיקבעו פעולות שיהיו תלויות באישור של הממונה. ניתן אף להוסיף חובת הנמקה לפעולות מסוימות המצריכות אישור הממונה. כך ניתן להפחית את הסיכון שתפקיד הממונה יהווה חותמת גומי ותו לא, ושמיומנותו וכשירותו יילקחו ברצינות במסגרת עבודת הארגון.

עם זאת, אנו סבורים שיש להשאיר את הליך הטמעת התפקיד כהליך אורגני, כחלק מהתרבות הארגונית של כל ארגון, ולא לכפות את החוק או הרגולציה לרמה מעשית לחיי היומיום של הארגונים השונים. לכן, ניתן לקבוע הוראות פחות פולשניות לחיי הארגון, כדוגמת חובות דיווח של הממונה למנכ"ל על פעולות במסגרת תפקידו, כך שהמנכ"ל יהיה חשוף לשיקולי פרטיות בעת קבלת החלטות בנוגע לפעולות מסוימות.

בחינת סנקציות

כאמור לעיל, האיחוד האירופי מצא כי ארגונים רבים, בכלל זאת ארגונים ציבוריים, לא מינו DPO למרות שהיו מחויבים לכך לפי הדין.¹¹² עולה מכך צורך בהעלאת מודעות לחובת המינוי, וכן צורך באכיפה במקרים של הפרות. כפי שנעשה ב-GDPR,¹¹³ רצוי לקבוע קנס על אי-ציות לחובת המינוי של ממונה הגנה על הפרטיות, או להוראות אחרות הנוגעות לפעילותו, כפי שיוטל קנס על אי-ציות לשאר המחויבויות מכוח החוק. כמו כן, רצוי שהקנס יוטל גם במקרים שבהם הממונה לא הוסמך לבצע את תפקידו מכוח החוק, כדי להימנע מניסיונות לעקיפת חובת המינוי על-ידי מינוי ממונה ללא יכולת אפקטיבית לבצע את תפקידו. לגבי חובות אחרות שקשורות למינוי של DPO, כמו חובה לפעול שלא בניגוד עניינים, ניתן לבחון סנקציות אחרות, כגון מתן סמכות לרשות להגנת הפרטיות לקבוע שהממונה פועל בניגוד עניינים, ולדרוש הזזה שלו מתפקידו ומינוי ממונה חדש במקומו.

לגבי הפרה של חובות על ביצוע תפקידו של ה-DPO והגדרת תפקידו – רצוי לשאוף שלא לקבוע הפרות במקרים שבהם הממונה אינו מבצע את תפקידו, שכן הגדרת תפקידו בארגון היא עניין מורכב שמשתנה מארגון לארגון. הטלת הקנסות על עצם אי-העמידה של הארגון כולו בהוראות חוק הגנת הפרטיות (שמטרתו של הממונה היא להקל ולוודא את העמידה בו) היא עדיפה על פני בחינה פרטנית של פעילותו של הממונה. בהקשר זה, בהתאם ל-GDPR,¹¹⁴ אנו מציעים שלא לקבוע אחריות אישית של הממונה על הגנת המידע בארגון.

¹¹¹ PIPEDA Self-Assessment Tool, לעיל ה"ש 89, תחת Principle 2 - Identifying Purposes בעמ' 10-13.

¹¹² [Designation and Position of Data Protection Officers](#), לעיל ה"ש 40, בעמ' 14-15.

¹¹³ סעיף 39(4)(a) ל-GDPR מאפשר הטלת קנס של עד 10 מיליון יורו או 2% מההכנסה השנתית של הארגון על הפרה של חובותיו מכוח סעיף 39 ל-GDPR, אשר עוסק בתפקידי ה-DPO.

¹¹⁴ סעיפים 37-39 ל-GDPR מטילים את החובות על מעבד המידע או הבעלים של מאגר המידע (controller or processor) ולא על ה-DPO באופן אישי.

4.1 סיכום שיקולים והמלצות

מינוי DPO : חיוב או המלצה?

ראוי לחייב מינוי ממונה הגנת פרטיות, במקרים המתאימים, באופן שישגי הגנה מירבית על פרטיות מבלי להעמיס עומס בלתי סביר על ארגונים. בתוך כך ניתן לשקול אפשרות שמחייבת מינוי בגופים מסוימים ומותרת לגופים אחרים את שיקול הדעת במינוי וולונטרי.

בעת קביעת המקרים בהם תחול חובת מינוי, השיקול המרכזי הוא הסיכונים לפרטיות. לכן יש להתחשב בעיקר בפרמטרים של רגישות המידע, היקף המידע ומספר נושאי המידע. בנוסף, יש לתת את הדעת גם למאפייני הארגונים עליהם נרצה להטיל את החובה (ציבורי, פרטי, מגזר שלישי).

ניתן לשקול אפשרות של מינוי ממונה אחד למספר חברות קשורות, ומינוי ממונה ממוקד חוץ לחברה.

הגדרת תפקיד

ראוי לקבוע הגדרת תפקיד כללית יחסית בחוק לצד פירוט נוסף בתקנות או הנחיות של הרשות להגנת הפרטיות. נמליץ שיהיה מדובר בתפקיד נפרד ומובחן ממונה אבטחת מידע.

בפרט לטעמנו יש לקבוע בחקיקה חובה שתוטל על הממונה לוודא את קיום הוראות חוק הגנת הפרטיות על ידי בעלים או מנהל של מאגר מידע, ולהגדיר כחלק מתפקידו הגברת המודעות לחשיבות הפרטיות והשלכותיה בארגון.

בנוסף, נמליץ להגדיר את הממונה להגנת הפרטיות כאיש קשר בנושא הפרטיות בארגון.

הגדרת ידע ומומחיות

יש לשקול האם לקבוע סטנדרט עמום בהגדרת הידע והמומחיות הנדרשים מהממונה להגנה על הפרטיות שיאפשר התאמה למאפייני וצרכי הארגון, או ליצור כלל ברור לשם יצירת רמת סף אחודה בקבלה והכשרה לתפקיד. נציע לשם שמירה על גמישות התאמת התפקיד לארגון לשלב ביניהם.

בנוסף, יש לבחון האם לחייב השתתפות בקורסי כשירות לשם קבלה לתפקיד ו/או ביצוע קורסי כשירות תקופתיים לשם עמידה ברמת כשירות ומומחיות אחידה. נמליץ להציע קורסי כשירות מטעם המדינה שיהיו זמינים חינם, מסובסדים או מפוקחים לשם הקלת הנטל על הארגונים השונים, ככל שהדבר מתאפשר מבחינה תקציבית.

עצמאות וניגוד עניינים

כדי לשמור על תפקיד הממונה להגנה על הפרטיות תפקיד עצמאי שניעדר ניגוד עניינים, מומלץ להגדיר מפורשות בחקיקה או בתקנות רשימה של תפקידים בארגון שהממונה לא יכול לכהן בהם במקביל לתפקידו. אפשרות חלופית היא אימוץ כלל רחב השומר על עצמאות וניגוד עניינים כנעשה ב-GDPR.

נמליץ לאמץ את הכלל הקבוע ב-GDPR לפיו אין להנחות את הממונה ביחס לפעילותו, ואין לפטר אותו או לפגוע בתנאי העסקתו בשל ביצוע תפקידו. זאת על מנת להבטיח שהממונה ישקול שיקולים ענייניים בעת ביצוע תפקידו, ולא יחשוש מפיטורים לא מוצדקים.

אחריות

נמליץ לשקול הוספת התייחסות מפורשת לאחריות הממונה בארגון על ציות להוראות החוק ואחריות למילוי בדומה לאחריות נושאי משרה מדיני החברות. יש לבחון כיצד ואם בכלל לייחד אחריות זו משאר

בעל התפקידים בארגון: דירקטוריון, ממונה על אבטחת מידע, בעל השליטה במידע ומעבד המידע. לחלופין ניתן לפטור ממונה מאחריות אישית בכלל או במקרים מסוימים.

שילוב תפקיד הממונה על הגנת הפרטיות בארגון

יש לשקול האם צריך להגדיר בפועל תמיכה של הארגון וההנהלה הבכירה בתפקיד הממונה, או להשאיר את התחום מחוץ להתערבות חקיקתית ורגולטורית.

במידה והוחלט להגדיר תמיכה בתפקיד להלן מספר חלופות מוצעות: מתן סמכות להתערב בהחלטות בארגון שנוגעות בנושאי פרטיות; התניית ביצוע פעולה או החלטה מסוימת בארגון שקשורה לעיבוד ושימוש מידע באישור של הממונה בארגון; הוספת חובת הנמקה לפעולות מסוימות המצריכות אישור ממונה; הוספת חובת דיווח של הממונה למנכ"ל על פעולות במסגרת תפקידו.

בחירת סנקציות

נמליץ על קביעת סנקציה כספית על אי-ציות לחובת מינוי ממונה או להוראות אחרות הנוגעות לפעילותו. נמליץ שהסנקציה תחול על הארגון כולו ולא כאחריות אישית על הממונה.

בנוסף נמליץ לתת סמכות לרשות להגנת הפרטיות לדרוש החלפת ממונה בארגון במקרים בהם הממונה לא פעל בהתאם לחוק.

5. סיכום

המגמה הגוברת של חיוב מינוי ממונה על הגנת פרטיות בארגונים היא מגמה מבורכת. אנו סבורים כי חיוב ארגונים למנות ממונה על הגנת פרטיות, במיוחד במקרים בהם הארגון מטפל במידע רב ורגיש, יתרום להגנה על פרטיות ולהגברת המודעות לחשיבותה. לאור חשיבות התפקיד, אנו ממליצים ליחד לו הגדרת תפקיד מפורשת ונפרדת מתפקיד ממונה על אבטחת מידע, וכן לנקוט במהלכים שיבטיחו את כשירותו של בעל התפקיד, עצמאותו בארגון ויכולת השפעתו.