



Shmilovich-Gruengard-Forshtat Law Offices

שמילוביץ-גרינגרד-פורשטט משרד עורכות דין

www.sgf.co.il • office@sgf.co.il

Clemy Shmilovich, LL.B Advocate & Notary
Galia Shmilovich Gruengard, LL.B Advocate
Lea Miller-Forshtat, LL.M Advocate & Mediator
Ruth Donner, LL.B Advocate & Notary
Meital Shapira, LL.B Advocate & Mediator
Gal Sade, LL.B Advocate

קלמי שמילוביץ, LL.B עורכת דין ונוטריון
גליה שמילוביץ גרינגרד, LL.B עורכת דין
לאה מילר-פורשטט, LL.M, עורכת דין ומגשרת
רות דונר, LL.B, עורכת דין ונוטריון
מיטל שפירא, LL.B, עורכת דין ומגשרת
גל שדה, LL.B עורכת דין

ינואר 2018,

שלום רב,

משרדנו בשיתוף עם אתי ברגר, דוקטורנטית ומומחית לתחום הסייבר, מלווה חברות וארגונים לקראת כניסתן לתוקף של חוק הגנת הפרטיות באיחוד האירופאי (GDPR) ותקנות הגנת הפרטיות (אבטחת מידע). שינויי החקיקה והרגולציה בתחום הגנת הפרטיות, הן באירופה והן בישראל, מהווים מהפיכה בתפיסת חובת ההגנה על הפרטיות ושמירה על המידע האישי. לא במקרה נכנסים לתוקפם גם החוק האירופאי וגם תקנות אבטחת המידע הישראליות במאי 2018 ולחקיקה של האיחוד האירופאי ישנה השפעה גם על חלק מהחברות והגופים הציבוריים בארץ.

במסמך זה ננסה לסקור את השינויים בחוק ולאפשר לכם הכרה כללית עם השלבים השונים בתהליך התאמת הארגון לדרישות החוק.

בחלקו הראשון של מסמך זה – "מהפכת ההגנה על פרטיות המידע" (עמ' 6-2):

תמצאו סקירה על שינויי החקיקה בתחום הגנת הפרטיות והמידע ואת עיקרי ההתאמות שעל כל ארגון המחזיק במאגר מידע לבצע בכדי לעמוד בתקנות החדשות ובכדי להמנע מזליגת מידע ומחשיפה לתביעות נזיקיות ופליליות.

בחלקו השני של המסמך – "התוכנית המודולרית של משרדנו" (עמ' 7 – 9):

תמצאו פרוט של שלבי התוכנית שיצרנו בשיתוף עם אתי ברגר בכדי ללוות את לקוחותינו בתהליך התאמת אבטחת המידע בארגון לדרישות החקיקה החדשות. התוכנית מאפשרת לכם להבין מהם השלבים השונים בתהליך ומהם הנושאים השונים הדורשים בדיקה והתאמה. התוכנית מתייחסת לדיסציפלינות השונות בארגון הדורשות בדיקה והתאמה ובכללן: היבטים טכנולוגיים, משפטיים ומנהלתיים.

להרחבה ומידע נוסף על הנושא – הטור השבועי של משרדנו במגזין אנשים ומחשבים

מוזמנים לקרוא את טור השבועי שלנו במגזין אנשים ומחשבים אשר מתפרסם בכל יום שלישי. לנוחיותכם, ריכזנו את הטורים שפורסמו עד כה במגזין אנשים ומחשבים באתר משרדנו:

[/https://sgf.co.il/from-the-media](https://sgf.co.il/from-the-media)

הנכם מוזמנים לפנות למשרדנו ולתאם פגישה לברור פרטני לגבי החובות החלות על החברה/ארגון שבניהולכם.

מבוא גרופית 4, ת"א 6930043 Grofit Alley Tel-Aviv

טל: 972-77-4020592 | פקס: 972-77-4020591 | www.sgf.co.il | office@sgf.co.il

חלק ראשון – מהפכת ההגנה על פרטיות המידע:

מבוא:

תקנות הגנת הפרטיות (אבטחת מידע) החדשות אינן סתם שינוי, אלא הן בגדר מהפיכה אמיתית בתחום הגנת הפרטיות והמלחמה בתקיפות סייבר וזליגת מידע פרטי. מזה מספר שנים שתחום הגנת הפרטיות, ניהול מידע אישי ואבטחת מידע נמצא במרכז הזירה והעדרן תקנות אחידות וברורות השפיע על פעילותם של חברות, ארגונים וגופים ציבוריים ועל אנשים פרטיים אשר הפקידו את פרטיהם האישיים בידי אותם ארגונים, מבלי שתהיה להם כל שליטה על השימוש במידע הפרטי והאישי שהפקידו ועל סיכוני הפגיעה.

איומי האבטחה והסייבר הלכו והתרבו, והפרצות בחקיקה המיושנת שהיתה קיימת עד כה, אפשרו זליגת מידע אישי ופרטי לצדדים שלישיים, והובילו לחשיפה ולניצול מידע אישי, בריאותי, פיננסי ורגיש ע"י אותם גורמים.

באיחור לא מבוטל נכנסו גורמי החקיקה והאכיפה ברוב העולם המערבי להליך חקיקה משמעותי ויסודי הנוגע לנושאי אבטחת מידע והגנה על פרטיות.

שיאו של ההליך הרגולטורי באירופה ובישראל יתרחש בחודש מאי 2018, אז ייכנסו לתוקף שתי חקיקות משמעותיות בנושא הגנת הפרטיות: תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017 שיחולו בישראל, ותקנות ה-(General GDPR Regulations Protection Data) שיחולו במדינות האיחוד האירופי וישליכו גם על מדינות אבטחת המידע במדינות שאינן חברות באיחוד האירופאי.

התקנות החדשות בישראל ובאירופה:

בישראל - תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017 (להלן: "התקנות"):

תחולנה על כל הגופים בישראל אשר מנהלים או מחזיקים מאגר מידע (רשום או שאינו רשום), כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 ("החוק").

התקנות חלות על כל הבעלים, המנהלים והמחזיקים של מאגרי מידע בישראל, כולל ארגונים, גופים, חברות, עסקים, בעלי מניות, דירקטורים, חברי ועד מנהל, נושאי משרה ואנשים פרטיים. כל אחד מאלו עשוי להיות חשוף אם לא יפעל כדין לפי התקנות.

התקנות מטילות חובות משפטיות, ניהוליות וטכנולוגיות ביחס לאבטחת המידע האישי השמור בחברה, ביחס ללקוחות, ספקים, עובדים או כל אחד אחר.

התקנות קובעות הסדר רחב ומקיף לעניין ההגנה על מאגרי מידע וניהולם, הן מבחינה טכנולוגית והן מבחינה משפטית. התקנות קובעות כללים ומנגנונים שמטרתם למנוע שימוש לרעה במידע, הן על ידי גורמים בתוך הארגון, והן על ידי גורמים מחוצה לו.

באירופה - ה-GDP (General Regulations Protection Data) הוא חוק הגנת

הפרטיות החדש:

החוק יחול במדינות האיחוד האירופי ויחול גם לגבי מידע על אזרחי האיחוד האירופי המוחזק בגופים מחוץ לגבולות האיחוד. חוק הגנת הפרטיות – GDPR יכנס אף הוא לתוקפו במאי 2018: השפעתן של תקנות ה-GDP רלוונטיות גם למדינות שאינן חלק מהאיחוד האירופי שכן הן חלות על כל גוף שמחזיק, אוסף או מעבד מידע אישי של אזרחי או תושבי האיחוד האירופי, בייחוד חברות המציעות מוצרים ושירותים דיגיטליים ואוספות תוך כדי כך מידע התנהגותי, רפואי, צרכני ופיננסי על אזרחי או תושבי האיחוד. חברה/ארגון שלא יצייתו להוראות החוק עלולות להיקנס בסכום של עד 4% מההכנסה השנתית הגלובאלית שלהן, או 20 מיליון יורו, הגבוה מביניהם, בהליך מנהלי מקוצר, ללא צורך באישור בית משפט, כאשר הפרה יכולה להיחשב כפלילית. בנוסף, חברות ישראליות עליהן חל החוק, עלולות להידרש להציג בפני לקוחותיהן ו/או שותפים עסקיים מאירופה, מסמך המעיד כי הן מצייתות לדרישות החוק, אחרת תיפסק ההתקשרות מולן.

מהו מאגר מידע לצורך תקנות אבטחת המידע?

חוק הגנת הפרטיות מגדיר "מאגר מידע" בתור: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב", כאשר "מידע" מוגדר בתור: "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". יש לשים לב כי הדרישה איננה מצטברת, היינו, גם מאגר שיש בו רק נתונים של שם ותעודת זהות של אדם, יכול להיות מאגר מידע לפי חוק. למעשה, הפרשנות המורחבת שניתנה לשאלה מהו מידע אישי, קבעה כי כל מידע שנאסף על אדם ואשר יאפשר זיהוי שלו, יוגדר ברוב המקרים כמאגר מידע ומאחר שכיום מאחר שכיום כמעט כל מידע שנאסף על אדם מאפשר זיהוי, גם אם מדובר במידע מאוד בסיסי ומיינמלי, אזי יהיה זה נכון לומר כי ברוב המקרים גם מאגר מידע עם מידע בסיסי יוגדר ככזה הכפוף לחוק והנחיות הקבועות בו.

אי עמידה בתקנות אבטחת המידע החדשות חושפות באופן אישי בעלי תפקידים

בארגון:

חשוב לומר, כי מעבר לאחריות הנזיקית אליה עלולים להיות חשופים בעלי המידע או מעבדי המידע שלא הקפידו על קיומן של התקנות, הרי שאי עמידה בהוראות התקנות מהווה למעשה עבירה על חוק הגנת הפרטיות, ולכן גוררת סכנה להטלת אחריות פלילית על הבעלים, העובדים ונושאי המשרה בארגון. עבירות על חוק הגנת הפרטיות נחשבות מן העבירות החמורות בספר החוקים, כאשר פגיעה בפרטיות באמצעים טכנולוגיים הפכה למכת מדינה, והמחוקק ובתי המשפט עושים כל שביכולתם להילחם בתופעה ולהחמיר עם העבריינים. עצם אי מילויין של חלק מהוראות התקנות מהווה עבירה פלילית מסוג אחריות קפידה, אשר מספיקה ההוכחה בדבר קיומה העובדתי של העבירה בלבד בכדי להרשיע בגינה, ללא כל צורך בהוכחה של יסוד נפשי של מודעות או רשלנות. העונש על עבירה כאמור, יכול להגיע עד שנת מאסר בפועל. כאשר מדובר בעבירות שנעברו במזיד, כמו שימוש במידע על ענייניו

הפרטיים של אדם שלא למטרה לשמה נמסר המידע או כאשר לא נשמרה סודיות המידע המצוי במאגר, מדובר בעבירה פלילית שהעונש עליה יכול להגיע עד 5 שנות מאסר. לאור כל האמור לעיל ולאור החשיבות העולה בכל הקשור לשמירה על פרטיותם של אנשים, המגמה בפסיקה תהיה החמרה עם אלו שייכשלו בעמידה בדרישות החוק והתקנות. על כן, המלצתנו היא לא ליטול סיכונים מיותרים וליישם את הוראות התקנות בהקדם.

התקנות החדשות מחייבות סיווג של מאגרי המידע לפי קטגוריות:

ככל שמדובר ב"מאגר מידע", יש לבחון לאיזו קטגוריה משתייך מאגר המידע, כאשר התקנות מחלקות את מאגרי המידע לארבע קטגוריות שונות, הנבדלות זו מזו ברמת ההגנות הנדרשות ממאגר המידע:

- **מאגר מידע המנוהל על ידי יחיד.** זה הוא מאגר שהגישה אליו נמצאת בידי לא יותר מ-3 אנשים, ובלבד שמטרתו אינה איסוף מידע לצורך מסירתו לאחר (כמו שירות דיוור ישיר), הוא אינו מכיל מידע על יותר מ-10,000 איש ואינו כולל מידע הכפוף לחובת סודיות.
- **מאגר מידע ברמת אבטחה בסיסית** (זו הגדרה שיווית – מאגר שאינו מוגדר כמנוהל על ידי יחיד ואינו נכנס לאחת הקבוצות הבאות של רמת אבטחה גבוהה יותר).
הרמות הבאות של אופי מאגרי המידע נמצאות בתוספות לתקנות – בתוספת הראשונה (רמת אבטחה בינונית) והשניה (רמת אבטחה גבוהה):
- **רמת אבטחה בינונית** מתייחסת למאגר מידע שמורשי הגישה אליו עולים של עשרה, שהוא בבעלות גוף ציבורי או גוף שממלא תפקיד ציבורי, שיש בו מידע רגיש. מאגר מידע של גוף ציבורי שמטרתו לאיסוף מידע לצורך מסירתו לאחר (לדוגמה: העברת המידע למשרד ממשלתי/גוף ציבורי שלו נדרש המידע לצורך ביצוע פעולות אשר בסמכותו לבצע) או כזה המכיל מידע רגיש, ובלבד שהוא מכיל מידע על 100,000 אנשים ומעלה או שמספר מורשי הגישה אליו עולה על 100.
- מידע רגיש יכול מידע מהסוגים הבאים: מידע על צנעת חיי האדם; התנהגותו של אדם ברשות היחיד; מידע רפואי או נפשי; מידע גנטי; מידע אודות דעות פוליטיות או אמונות דתיות; על עבר פלילי; נתוני תקשורת; מידע ביומטרי; מידע על נכסיו, חובותיו והתחייבויותיו של אדם; הרגלי צריכה של אדם וכדומה.
- **רמת אבטחה גבוהה** מתייחסת למאגר כאמור ברמת האבטחה הבינונית, שיש בו מידע על 100,000 איש ומעלה או שמספר מורשי הגישה אליו עולה על 100.
- תוכן המידע במאגר קובע רק חלק ממידת האבטחה הנדרשת ויש חשיבות רבה גם להיקפו ולמידת הנגישות של אנשים אל המידע שבו. גם הם משפיעים על מידת האבטחה הנדרשת בכל מאגר.

השלבים השונים הנדרשים לצורך התאמת אבטחת מאגרי המידע על פי התקנות

הישראליות:

המחוקק קובע את הצעדים שעל בעל מאגר מידע לנקוט לשם הגנה על המאגר ומניעת הפרת הפרטיות של נשואי המידע. למשל: אילו מסמכים עליו להכין, איזה תיקונים עליו להכיל על מסמכיו המשפטיים ועל ההתקשרויות שלו עם גורמים שונים. כמו כן קובע המחוקק שורה של נהלים שעל בעל המאגר לנסח ולהטמיע בארגון, מול אילו תרחישים עליו להתמודד, אלו תוכניות עליו להכין, חובתו למפות את מאגר המידע שלו, חובתו לסקור את הסיכונים ואפשרויות החדירה למאגר המידע ודרכי ההתמודדות מולם, חובתו לעקוב אחר השינויים המתרחשים בנושא, ועוד. לא כל החובות חלות על כל סוגי המאגרים אלא יש לקיימן בהתאם לסוג המאגר. מכאן חשיבותו של שלב "סיווג המאגר" ומיפוי המידע השמור בו, שהוא השלב הראשון בתהליך (כמפורט להלן בחלקו השני של מסמך זה). לאחר סיווג המאגר על החברה/ארגון לערוך את "רשימת הפערים" אשר תגדיר מהן המשימות שעל הארגון לבצע בכדי לעמוד בתקנות הפרטיות החדשות. בעזרת "רשימת הפערים" וסדרי הפעולות הרלוונטיות יתאפשר לארגון לערוך תוכנית עבודה מסודרת ולקבוע את המועד בו היא מעריכה כי תוכל לעמוד בדרישות התקנות החדשות. נציין כי, לעניות דעתנו, סביר להניח שחברה אשר תחל פעילות ראויה לצורך התאמת דרישות האבטחה של מאגר המידע שלה לתקנות החדשות תיטול על עצמה סיכון נמוך יותר לקנסות ולתביעות גם אם לא תהיה מוכנה באופן מלא במאי 2018, בעוד שחברה אשר לא תפעל להסדרת ההגנה על מאגרי המידע שלה לקראת מאי 2018, תחשוף את עצמה לתביעות ולקנסות חמורים בהרבה. חשיפה זו תהיה רלוונטית בייחוד לנושאי המשרה, בעלי המניות והדירקטורים אשר פעלו ברשלנות ונמנעו מלהתאים את תנאי אבטחת המידע בארגון לתקנות החדשות.

להלן בראשי פרקים עיקרי השלבים הנדרשים לצורך התאמת דרישות אבטחת המידע בארגון

לתקנות החדשות:

- ניסוח מסמך הגדרות מאגר – יש לנסח מסמך הגדרות מאגר הכולל תיאור כללי של פעילות איסוף ושימוש במידע, מטרות השימוש, פרטים על העברת מאגר המידע אל מחוץ לישראל, ועוד. המסמך יעודכן בכל שינוי משמעותי ונחיצות השמירה של המידע תיבדק אחת לשנה.
- נוהל אבטחה – ינוסח מסמך נוהל אבטחת מידע אשר יכלול, בין היתר, הוראות בעניין אבטחה פיזית וסביבתית של אתרי המאגר, הרשאות גישה למאגר, תיאור אמצעי אבטחה על מערכות המאגר, הוראות למורשי הגישה ועוד.
- מיפוי מערכות וסקר סיכונים - יוחזק מסמך מעודכן של מבנה המאגר אשר יכלול, בין היתר, פרטים אודות תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע, מערכות התוכנה המשמשות להפעלת מאגר המידע ועוד.
- יישום ותייעוד של אמצעי אבטחת מידע, לרבות אבטחה פיזית וסביבתית, אבטחת תקשורת של המאגר, גיבוי ושחזור, וכיוצ"ב.

- תיעוד אירועי אבטחה - תיעוד כל אירועי האבטחה בקשר עם מאגר המידע. התקנים ניידים - בעל מאגר המידע יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר או ינקוט אמצעי הגנה.
- מיקור חוץ - התקנות קובעת הוראות לעניין התקשרויות מול גורמים חיצוניים שונים לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע.
- התקנות מאפשרות לרשם מאגרי המידע לפטור מאגר מסוים מחובות אבטחת המידע או להחיל על מאגר מסוים חובות אבטחה, לפי נסיבות העניין. פניה לרשם לצורך בקשת פטור כאמור תבחן בכל ארגון בנפרד ותוגש במידת הצורך בצירוף חוות דעת משפטית ודוח טכנולוגי תומך.
- הנחיות ספציפיות של הרשם לגבי מאגרי מידע אשר המידע השמור בו, חלקו או כולו מוגן בתקן אבטחת מידע רלוונטי.
- התקנות קובעות חובת דיווח לרשם מאגרי המידע על אירועי אבטחת מידע חמורים.
- התקנות כוללות חובה להקים וליישם מנגנונים פנים ארגוניים שיאכפו את עקרונות אבטחת המידע, והדגשת חובותיהם ואחריותם של מנהלי ובעלי מאגרי המידע.

ונדגיש – זו היא רשימה כללית אשר מתייחסת לכל סוגי המאגרים ואין להסיק ממנה לגבי

הפעולות הנדרשות בארגונכם, שכן לא כל החובות המפורטות להלן חלות על כל סוגי

המאגרים



Shmilovich-Gruengard-Forshtat-Donner Law Offices
משרד עורכות דין שמילוביץ-גרינגרד-פורשטט-דונר

7

חלק שני – התוכנית המודולרית של משרדנו:

מטרת התוכנית: התאמת רמת אבטחת המידע בארגון כנדרש בחקיקה תוך התחשבות בצרכים, ובמשאבים של הארגון

שיתוף הפעולה המשפטי-טכנולוגי שיצרנו מאפשר לנו ללוות את חברות וארגונים בכל השלבים הרלוונטיים עד להתאמה מלאה של מאגרי המידע לדרישות החדשות. התוכנית מודולרית שלפניכם מותאמת לכל לקוח כתלות בסיווג מאגרי המידע שברשותו בהתאם לקריטריונים הקבועים בתקנות. ייחודה של התוכנית הינו בכך שהיא מאפשרת ללקוחותינו לבחור את סוג הליווי הנדרש עבורם בכל אבן דרך, החל מליווי מלא ושימוש בכל הכלים שבארגז הכלים של משרדנו וכלה בליווי נקודתי לצורך הנחיה והדרכה שלנו את צוות הארגון שמבצע את היישום בפועל של ההתאמות. אנו מאמינות כי נוכל לפשט עבורכם את הדברים וכי לאחר סיום אבן הדרך הראשונה (כמפורט להלן) תהיה בפניכם כל האינפורמציה ותהיה ביכולתכם כמקבלי ההחלטות בארגון היכולת לבחור כיצד לבצע את תהליך התאמת אבטחת המידע. חוות הדעת שנמסור לידיכם עם סיום אבן הדרך הראשונה תקנה לכם הכרה עם התקנות ושליטה על ניהול התהליך בהתאם לתקציב ולמשאבים העומדים לרשות הארגון.

אבני הדרך בתוכנית המודולרית:

אבן דרך ראשונה - אפיון וסיווג המידע שנאסף בארגון: סיווג מאגרי המידע שנאסף בארגון, מיפוי הדרכים בהן נאסף המידע, זיהוי ומיפוי נכסי מידע ארגוניים, מיפוי התהליכים הידניים ו/או האוטומטיים אשר באמצעותם מעבדים, אוספים או מאחסנים מידע אישי, מיפוי הדרך בו עושה הארגון שימוש במידע לצורך פעילותו. בתום אבן הדרך הראשונה יוגש לארגון דו"ח דרישות מאגר מידע הנתמך בחוות דעת משפטית המסכמים את סיווג רמת המידע, מאגרי המידע ונכסי המידע האירגוניים שדורשים הגנה על פי התקנות.

חוות הדעת המשפטית מגבה את הדו"ח הטכנולוגי בהיבטים משפטיים, מתקפת את תהליך הבדיקה, קביעת הסיווג וקביעת נכסי הארגון הדורשים הגנה על פי חוק (להבדיל מנכסי חברה אשר יקבע לגביהם שאינם כפופים לחוק ולדרישות). הדוח שיוגש בתום אבן הדרך הראשונה יאפשר למנהלים בארגון לשקול איזה מאגרים ברצונם



להמשיך ולשמר, האם נכון יהיה לשלב מאגרים שונים וע"י כך ליעל את השימוש במידע ולחסוך עליות בניהול הגנת אבטחת המידע ויאפשר לנו כגורם המקצועי להכין תוכנית עבודה להמשך הליווי תוך התייחסות לסדרי עדיפויות בביצוע התהליך ביחס לסיווגים השונים של מאגרי המידע ולנקודות תורפה פוטנציאליות שנזהה כבר בשלב המיפוי.

אבן דרך שניה: מיפוי טכנולוגי והכנת דוח הערכת סיכונים בהתאם לדרישות החוק. בשלב זה יתבצע תהליך הערכת הסיכונים, זיהוי סיכונים, איתור נקודות תורפה, והתייחסות לסבירות להתרחשות אירוע סייבר והשפעת האירוע על הארגון. ההתייחסות בהערכת הסיכונים הינה גם כלפי סיכונים פנים ארגוניים (מבדקים פנימיים, וסקרי הנהלה) וגם חוץ ארגוניים. בחינה וסקירה מקיפה של אמצעי אבטחת המידע בארגון כנגד סיכונים, כגון: אובדן מידע, חדירה למערכת, וירוסים, כניסות בלתי חוקיות למערכת ואף שיחזור המערכת. בסופה של אבן הדרך השניה ימסר לארגון דוח הערכת הסיכונים מפורט.

אבן דרך שלישית: מיפוי נהלים ומסמכים נלווים בארגון ועריכת נוהל דוגמה לדיווח אירוע דליפת מידע מותאם לארגון (בהתאם לדרישת התקנות) : שלב זה יכלול סקירת מסמכי מדיניות הארגון, הסמכים של הארגון אשר יש להם רלוונטיות להיבטי איסוף מידע ושימוש בו, הסמכים מול ספקים, לקוחות ועוד אשר בהתקשרות מולם ישנה התייחסות לאיסוף מידע ושימוש בו, הכנת כל הנהלים הרלוונטיים לצורך קביעת הדרכים לאבטחת המידע ולגורמים המורשים לגשת למידע. כמו כן בשלב זה יבדקו המסמכים הנלווים של הארגון הנוגעים לאיסוף מידע כדוגמת: רישום למערכת הדברור של הארגון, תקנונים באתרי הרשת, רישום לרשת אלחוטית של גורמים המבקרים בארגון ועוד. כמו כן, בשלב זה תתבצע עריכת נוהל דוגמה לדיווח אירוע דליפת מידע מותאם לארגון (בהתאם לדרישת התקנות). שלב זה מתבצע ככל האפשר במקביל לאבן הדרך הרביעית ועל כן בדרך כלל דו"ח מסכם של המסמכים, הנהלים והחוזים של הארגון הדורשים עדכון ימסר ביחד עם הדו"ח המסכם של שלב 4. לארגונים המלווים ע"י יועץ משפטי קבוע יוכלו להעביר את רשימת המסמכים הנדרשת לטיפולו. בארגונים שאין להם ליווי משפטי קבוע, ניתן להעזר בשרותי משרדנו לצורך ביצוע עדכון החוזים, הנהלים והמסמכים הנלווים.



Shmilovich-Gruengard-Forshtat-Donner Law Offices
משרד עורכות דין שמילוביץ-גרינגרד-פורשטט-דונר

אבן דרך רביעית: הכנת מסמך מסכם, המתאר את ניתוח הפערים בין המצב הקיים לבין החובות החלות על החברה מכוח התקנות. המסמך יכלול פרוט מלא של כל הנושאים הדורשים טיפול של הארגון וישלב את הפרוט בתוכנית עבודה שתוגש לארגון ליישום ההמלצות. תוכנית העבודה תתייחס גם לתעדוף המשימות בהתאם למידת הדחיפות והחשיבות של המשימה. הדוח כאמור יאפשר לחברה לקדם את כל הנושאים אשר ביכולתה לקדם ללא ליווי שלנו. דוח הפערים יתמך בחוות דעת משפטית.

אבן דרך חמישית: ביצוע הדרכה אחת מקיפה לנושאי התפקידים המתאימים בארגון אשר אמונים על יישום מדיניות אבטחת המידע וניהול המידע האישי בארגון, על מנת להסביר את המדיניות החדשה, והדרכתם בדבר השלמת המדיניות באופן עצמאי.

אבן דרך שישית: ככל שהארגון ידרש לליווי נוסף הוא יוכל להעזר בשרותינו לביצוע משימות נוספות כגון: בניית מדיניות אבטחת מידע, ניסוח מסמך הגדרות המאגר ומינוי ממונה על אבטחת מידע. ניסוח מסמך סיכוני פגיעה במאגר, כתיבת נהלים, עריכת שינויים במסמכי החברה, הכנת מסמכי מדיניות, כללי התנהגות ונוסחי הודעות, אמנות שירות ועוד. ליווי הארגון בתהליך ההטמעה של מדיניות אבטחת המידע, קיום סדנאות הדרכה ארגוניות וסיוע בניהול התהליכים הכרוכים בעמידה בהוראות החוק וקביעת בדיקות תקופתיות כנדרש בתקנות. לרוב, בשלב זה, הארגון בשל לפעול באופן עצמאי בהנחיית הממונה על אבטחת המידע שמינה הארגון ונעזר בשירות שלנו רק לצורכי הנחיה ו/או ליווי משפטי ככל שלארגון אין יועץ משפטי קבוע.

**נשמח לעמוד לרשותכם,
משרד עורכות הדין SGFD בשיתוף עם אתי ברגר**