ת.צ. 5077-12-20

בית המשפט המחוזי

<u>המחוז מרכז</u>

בעניין:

יהודה חכם ת"ז 051884955

בית המשפט המחוזי מרכז - לוד
2 -12- 2020
(84) התקבל (84)

עו"ד יוחי גבע
מרחוב דרך מאיר ויסגל 2, פארק המדע
רחובות, 76326
טל. 08-9102344 פקס: 08-9102361

(להלן: "**המבקשים התובעים**");

- נ ג ד -

שירביט חברה לביטוח בע"מ ח.פ. 512904608

יד חרוצים 18, נתניה

(להלן: "**המשיבה הנתבעת**");

<u>מהות הבקשה</u>- בקשה להכרה בתובענה כייצוגית, כספית נזיקית ולמתן צווים

<u>הסעד האישי המבוקש</u>- לכל אחד ואחד מחברי הקבוצה **1500** ₪

<u>הסעד הקבוצתי</u>- **600,000,000** ₪ (הערכה בלבד)

<u>בקשה לאישור תובענה ייצוגית</u>

בהתאם לחוק תובענות ייצוגיות, תשס"ו- 2006

בקשה לאישור תובענה ייצוגית

המבקש מתכבד בזאת, להגיש לבית המשפט הנכבד, בד בבד עם הגשת התביעה העיקרית בתיק דנן (**"התביעה"**), בקשה לאישור התביעה כייצוגית לפי הוראות חוק תובענות ייצוגיות, התשס"ו-2006 (להלן: **"חוק תובענות ייצוגיות"**).

- כתב התביעה מצ"ב **כנספח "1"** לבקשת האישור.
- תצהיר המבקש, מצ"ב **כנספח "2"** לבקשת האישור.

הגדרת הקבוצה: בית המשפט הנכבד מתבקש בזאת לאשר את ניהול התובענה בשם קבוצת הצרכנים הבאה:

"כל אדם או אישיות משפטית אחרת, אשר הפרטים שלהם נכללו במאגר המידע של שירביט, ונחשפו, כתוצאה מהארועים הקשורים בדיווח של רשויות הביטוח והסייבר ו/או כל המבוטחים אשר הפרטים שלהם כלולים במאגר המידע של שירביט ואשר סבלו ו/או יסבלו מעוגמת נפש כתוצא מפרסום דבר פרשת דליפת המידע ו/או כל המבוטחים אשר הפרטים האישיים שלהם נכללו במאגר המידע של שירביט, והמידע השמור נפגם כולו או חלקו"

"ביסוד התובענה הייצוגית מונחים שני שיקולים מרכזיים: האחד, הגנה על אינטרס הפרט באמצעות מתן תרופה ליחיד שנפגע. אותו יחיד, ברוב המקרים, אינו טורח להגיש תביעה. לעתים בא הדבר בשל כך שהנזק שנגרם לאותו יחיד הוא קטן יחסית. עם זאת, הנזק לקבוצה הוא גדול, כך שרק ריכוז תביעות יחידים לתביעה אחת, היא התובענה הייצוגית, הופך את תביעתם לכדאית...", "...השיקול השני עניינו אינטרס הציבור. ביסוד אינטרס זה מונח הצורך לאכוף את הוראות החוק שבגדריו מצויה התובענה הייצוגית..."

דברי הנשיא (לשעבר) ברק ברע"א 4556/94 טצת נ' זילברשץ, פד מט(5) 776.

א. מבוא:

א.1. תמצית התובענה בקיצור נמרץ

1. המשיבה הנה חברה ביטוח, ולה כ- 1,000,000 לקוחות.

2. ביום 1.12.20, הודיע רשות שוק ההון, ביטוח וחיסכון ומערך הסייבר הלאומי, שהאקרים פרצו לאתר ולשרתי המשיבה.

העתק מהודעת מערך הסייבר הלאומי, מצ״ב ומסומן: ״3״.

3. כתוצאה מן הפריצה, הועברו פרטים רבים של לקוחות המשיבה, לידי ההאקרים, ורבים מהם, אף פורסמו ברשת.

4. כל למשל פורסמו, רשיונות נהיגה, תעודות זהות, תביעות ביטוח, תלושי שכר , קרנות השתלמות קרנות פנסיה, ועוד פרטים רבים ביותר של לקוחות החברה.

5. ההאקרים מקבוצת BlackShadow, שפרצו לשרתי המשיבה, אמרו לעיתונאים בישראל, כי ברשותם יש טרות (אלפי גייגה-בייט) של מידע, וכי בכוונתם למכור את פרטי הלקוחות שדלפו. במסמכים שדלפו, נראים בין היתר גם כמה מסמכים על היעדר עבר ביטוחי הכוללים שמות מלאים, כתובות, ותעודות זהות.

6. הדלפת המסמכים נמשכה אף בלילה שלאחר מכן.
קבוצת ההאקרים קיבלה אחריות על הפריצה לשרתי החברה, ופרסמה בחשבונות הטוויטר והטלגרם שלה פרטי לקוחות ומסמכים בהיקף עצום, משנת 2012 ועד שנת 2020. תחילה הנפח של אותם פרטים נאמד ב-929 גייגה-בייט, אך לדבריהם מדובר באלפים. על פי הערכות, מדובר במידע של מאות אלפי מבוטחים, ולעיתים הוא כולל מספרי תעודות זהות - המשמשים בגופים רבים, גם ממשלתיים, כאמצעי אימות משני. לפני פחות מחודש זכתה שירביט במכרז לביטוח רכב פרטי לעובדי מדינה בשנת 2021, ומבוטחים בה רבים המשרתים בכוחות הביטחון.

בין ההקלטות שפורסמו בעמוד הטלגרם של התוקפים, ישנה שיחה עם לקוחה, מספר תעודת הזהות שלה ופרטי התאונה שעליה דיברה עם החברה. בנוסף, פורסם מייל ובו פרטי כרטיס אשראי.

צילום מקצת החומרים האישיים שהודלפו לרשת (לרבות של כבוד השופט גלעד נוייטל), מצ״ב ומסומן: ״4״.

7. לתדהמת לקוחות המשיבה, הוברר בתקופה האחרונה, כי המשיבה הפרה את חוק הגנת הפרטיות, תקנות הגנת הפרטיות את ההסכמים עם לקוחותיה, וחובות נוספים, בכך, שבשל התרשלותה, והפרת חובותיה, עת היא לא שמרה על פרטי לקוחותיה, ואלו היום חשופים לכל, פשוטו כמשמעותו.

8. למעשה, בשל פירצת האבטחה המורה ביותר שניתן לדמיין, וחולשות האבטחה החמורות שהובררו שקיימות במערכות ובשרתי המשיבה, כמו גם, בשל בשל רשלנותה של המשיבה, הרי שכל המידע האישי של הלקוחות, בשמם המלא, כתובתם, מספרי הטלפון שלהם, מספרי הזהות שלהם, מספרי חשבונות הבנק שלהם, ספרות אחרונות בכרטיסי האשראי של הלקוחות, ועוד מידע רב - נחשף, והכל כפי שהיה מצוי בבמאגר המידע של המשיבה.

9. בהתאם לאמור, מובן שהמשיבה, לא טיפלה בהתאם לחובתה, בנושאי אבטחת המידע, הנוגעים לפרטי לקוחותיה, לרבות כל המידע דלעיל, ולמעשה הפקירה את פרטיות לקוחותיה.

10. בשל כך, תרמה המשיבה לחשיפת מידע בהיקף רחב ביותר, וברמות רגישות גבוהות, תוך שהיא התעלמה מסיכון זליגת המידע, מתוך החברה ומחוצה לה, וביצוע השימוש במידע, מעבר למטרות שלשמן נשמר המידע.

11. זאת ועוד, המשיבה פרסמה הודעה ללקוחותיה, אשר מלמדת כי היא איננה מבינה את עוצמת הנזק שנגרם ללקוחותיה.

12. בכך הפרה המשיבה, את חובותיה, האמורים בסעיף 17 לחוק הגנת הפרטיות, התשמ"א – 1981, ובכך העמידה בסיכון ממשי, את מליון לקוחותיה.

13. בנוסף, הפרה המשיבה את תקנות 2, 4, 5 (א), 9 (ב)(2), 10, 11 (S) ו- 14 (א), לתקנות אבטחת המידע.

14. זאת ועוד, ביום 31.8.16, פרסמה הממונה על שוק ההון ביטוח וחיסכון, הגב' סלינגר, חוזר לגופים מוסדיים 2016-9-14, תחת הכותרת "ניהול סיכוני סייבר בגופים מוסדיים".

העתק החוזר, מצ"ב ומסומן: "5".

15. הוראות החוזר, אינן משתמעות לשתי פנים.

16. המשיבה הפרה אף את הוראות החוזר.

17. כתוצא ממחדלי המשיבה, הרי שפרטי לקוחותיה, לרבות המידע האישי של הלקוחות, שמם המלא, כתובתם, מספרי הטלפון שלהם, מספרי הזהות שלהם, מספרי לוחיות הרכב שלהם, מספרי שלדות הרכב שלהם, חשבוניות הלקוחות, מספרי חשבונות הבנק שלהם, ספרות אחרונות בכרטיסי האשראי של הלקוחות, היו פרוצים לכל, והכל כפי שהיה מצוי בבמאגר המידע של המשיבה.

18. אך מובן, כי כתוצאה מההפרה, נגרמו לחברי הקבוצה, נזקי, הן ממוניים והן בלתי ממוניים, לרבות העמדה בסיכון ממשי – לרבות נזק כלכלי.

19. עוד מובן, כי המשיבה הפרה את הוראות הדין כמו גם הוראות חוק חוזה ביטוח, תקנות הביטוח שלפי החוק, והוראות הרגלוטור ביחס לחובותיה כלפי לקוחותיה כמבטחת.

20. עוד הפרה המשיבה, את ההסכמים כלפי לקוחותיה, עת נכשלה בכישלון חרוץ, בשמירה על המידע האישי של לקוחותיה, ואשר נמסר לה על ידיהם.

21. התנהגות המשיבה, איננו מתקבל על הדעת, ומהווה פגיעה חמורה בפרטיות של חברי הקבוצה.

22. עוד מהווה התנהגותה, הטעיה והתרשלות, הפרת חובה חקוקה והפרת הסכם כלפי חברי הקבוצה.

23. בנסיבות אלו, אין מנוס מהגשת תובענה ייצוגית מוצדקת זאת, על מנת לזכות את חברי הקבוצה בפיצוי המגיע להם, בשל הפגיעה בפרטיותם, וכן בשל ההטעיה וההתרשלות כלפיהם.

24. חוק תובענות ייצוגיות, עוד בסעיף 1 לחוק, מגדיר כי הוא נועד :
"לשם שיפור ההגנה על זכויות".

1. זכות בסיסית מרכזית, הטעונה שיפור ובאופן דחוף, היא זכותו של האדם בכלל, ולקוחותיהם של המשיבה בפרט, **לפרטיות**. מדובר בזכות חוקתית כחלק מזכותו של האדם לכבודו. כפי שנקבע בע"פ **5026/97 גלעם ואח' נ' מדינת ישראל**, דינים עליון נו 164 :

"הנה כי כן : הזכות לפרטיות היא, בין היתר, אחת הנגזרות של הזכות לכבוד. הכרה בפרטיות היא ההכרה באדם כפרט אוטונומי הזכאי לייחוד אל מול האחרים. ייחוד זה הוא המאפשר לאדם להתבצר באישיותו כבעלת משמעות הראויה לכיבוד. פרטיותו של אדם היא כבודו וגם קניינו. זוהי המסגרת באמצעותה הוא עשוי ם הוא בוחר בכך. לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בתנהגותו ובמעשיו הפרטיים. זהו "מבצרו" הקנייני, האישי והנפשי".

2. זכות זו נרמסת באופן גס בידי המשיבה, להבדיל ממתחריה בשוק, בניגוד מוחלט להוראות הדין ולהראות הרגולטור, אשר לדאבון הלב אינן נאכפות.

3. עסקינן, כאמור, בהתרשלות רבתית, באבטחת מידע רגיש ביותר, של הלקוחות, דבר אשר חשף את פרטיהם האישיים.

4. לאור נסיבות התנהלות המשיבות כאמור לעיל ולהלן, נטען כי למעשה קשה לחשוב על מקרה מובהק יותר, המצדיק הגשת תובענה ייצוגית. על המשיביה יהיה לפצות את לקוחותיהם אשר פרטיותם נפגעה. כן יתבקשו צווים שתכליתם למנוע את המשך הפרת הוראות הדין. על כל להלן.

א.2. על הזכות לפרטיות

5. הזכות לפרטיות בע"פ **5026/97 גלעם ואח' נ' מדינת ישראל**, דינים עליון נו 164 :

"הנה כי כן : הזכות לפרטיות היא, בין היתר, אחת הנגזרות של הזכות לכבוד. הכרה בפרטיות היא ההכרה באדם כפרט אוטונומי הזכאי לייחוד אל מול האחרים. ייחוד זה הוא המאפשר לאדם להתבצר באישיותו כבעלת משמעות הראויה לכיבוד. פרטיותו של אדם היא כבודו וגם קניינו. זוהי המסגרת באמצעותה הוא עשוי ם הוא בוחר בכך. לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בתנהגותו ובמעשיו הפרטיים. זהו "מבצרו" הקנייני, האישי והנפשי".

6. וכך גם נקבע **בע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' אריה ורדי** (23/01/2013 פורסם בנבו) בפסקה 22 לפסק דינו של כב' השופט פוגלמן :

"הזכות לפרטיות היא מהחשובות שבזכויות האדם בישראל. היא אחת החירויות המעצבות את אופיו של ההמשטר בישראל כמשטר דמוקרטי...ממועד קבלתו של חוק יסוד : כבוד האדם וחירותו, אף מוקנה לה מעמד חוקתי (ס' 7 לחוק היסוד) הפרטיות מאפשרת לאדם לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בהתנהגתו ובמעשיו הפרטיים. היא "מבצרו" הקנייני, האישי והנפשי"... הזכות לפרטיות, אם כן, מותחת את הקו בין הפרט אל הכלל, בין האני לבין החברה. היא משרטטת מתחם אשר בו מניחים את הפרט לנפשו לפיתוח האני שלו. בלא מעורבות של הזולת... היא "מגלמת את האינטרס היחיד שלא להיות מוטרד בצנעת חייו על ידי אחרים"

ראה בנוסף **רעא 4447/07 רמי מור נ' ברק אי טי סי(1995) החברה לשרותי בזק בינלאומיים בע"מ** (25/03/2010, פורסם בנבו) פסקה 13 לפסק דינו של המשנה לנשיא ריבלין :

7. הזכות לפרטיות אינה מתמצה בזכותו של האדם לנהל את חייו בביתו שלו ללא חדירה לפרטיותו, ויש להבינה ולעבדה באופן רחב יותר. כזכותו של האדם "להעזב לנפשו". יפים בהקשר זה דבריו של השופט גרוניס בבג"צ **8070/90 האגודה לזכויות האזרח בישראל נ' משרד הפנים ואח'** בפסקה 2 :

"ישתי פנים לה לזכות הפרטיות הנזכרת בסעיף 7א לחוק יסוד כבוד האדם וחירותו. הפן האחד שניתן למצוא מקרי בכבוד האדם, הינו "זכותו של אדם לנהל את אורח החיים שבו הוא חפץ בדל"ת אמות ביתו, בלא הפרעה מבחוץ" (בג"צ 2481/93 דיין נ' ניצב יהודה וילק, פ"ד מח(2) 456, 470 וכן ראו ע"פ 1302/92 מדינת ישראל נ' נחמיאס, פ"ד מטב 309,353) ***<u>אין להוביל אמירה זו להביט הפיזי של הבית.</u>***

<u>יש להבינה בצורה רחבה יותר, באופן מטפורי ברוח הביטוי שטבעו וורן וברנדייס " the right to be left alone" (s.d warren & l.d brandies "the right to privacy" 4 harv. L. rev 193 (1980)."</u>

8. נעלה מכל ספק, כי הזכות לפרטיות ראויה להגנה, הגנה חוקתית, והן הגנה במסגרת אכיפת הוראותיו של חוק הגנת הפרטיות. מיותר לציין, כי כלי התובענה הייצוגית הנועד לשם שיפור ההגנה על זכויות כמו גם אכיפת הוראות הדיוף הינו המתאים גם לשם שיפור תמונת המצב העגומה בניפי המשיבים – כפי שתפורט להלן.

9. דומה כי קשה לחשוב על מקרה מובהק יותר של פגיעה בפרטיות, מאשר גניבת מידע כלכלי – אישי פרטי של אדם, מקום בו, המשיבה מחזיקה במאגר מידע, המכיל, פרטיו האישיים של אדם, מספר כרטיס האשראי שלו ועוד.

10. לא יתכן, כי חברה, העושה שימוש, בפרטי נכסים של אדם, לרבות רכבו, כרטיסי אשראי, בהם יכול אדם לרכוש מהונו האישי, וחשבון הבנק שלו, והכל באמצעות מספר כרטיס האשראי ופרטים נוספים (לרבות מספר זהות, שם ועוד), תתרשל כלפי אותו אדם, ולא תאבטח באופן מוחלט, ובהתאם לדרישות ממנה – את אותם פרטים – המצויים באותו מאגר מידע.

<u>יצירת מאגר מידע</u>

11. מעבר לפגיעה בפרטיות , הרי שסעיף 7 לחוק הגנת הפרטיות מגדיר המונחים "מאגר מידע" ו- "מידע רגיש" באופן הבא :

*"**מאגר מידע**" - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט–*

(1) אוסף לשימוש אישי שאינו למטרות עסק ; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף ;

מיום 11.4.1996 תיקון מס' 4

ס"ח תשנ"ו מס' 1589 מיום 11.4.1996 עמ' 290 (ה"ח 2234)

*"**מאגר מידע**" – מרכז להחסנת מידע באמצעות מערכת עיבוד נתונים אוטומטית אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט -*

(1) אוסף לשימוש אישי שאינו למטרות עסק ; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף ;

"מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו ;

*"**מידע רגיש**" –*

(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו ;

(2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

12. לענייננו, לא תיתכן מחלוקת כי המשיבים יוצרים מאגר מידע של ממש, ובו מידע רגיש כפי שקובעות הנחיות הרשות להגנת הפרטיות החל מסעיף 2.7 ואילך:

7.2 "לפי הגדרות המונחים" מידע "ו"מאגר מידע "בסעיף 7 לחוק ,התחולה של פרק ב 'בחוק היא על שמירת נתונים על אודות אדם ,באשר המידע אודותיו מזוהה או ניתן לזיהוי. לנוכח מאפייניהן המפורטים לעיל ,חלק ניכר מן החקלטות ממצלמות המעקב הקיימות כיום נכנס לגדר" מאגר מידע " המתייחס למידע מזוהה ,או ניתן לזיהוי ,אודות אדם ,כמשמעותו בסעיף 7 לחוק בין אלה כלולות:

13. מסקנות הדברים, שוב נזכיר, היא כי שימוש במצמות המעקב גורם ליצירת מאגר מידע, כמשמעותו בהוראות סעיף 7 לחוק הגנת הפרטיות. בענייננו – מדובר אף במדיע רגיש. 3

14. אך מובן, כי המשיבה אוחזת במאגר מידע, הכולל פרטי כרטיסי האשראי, שם ומספר תעודת זהות של לקוחותיה, ופרטים רבים נוספים.

<u>פגיעה בפרטיות:</u>

15. סעיף 17 לחוק הגנת הפרטיות מורה כך:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

16. 17א. (א) מחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר.

17. (ב) מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

18. 17ב. (א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - הממונה):

19. (1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

20. (2) גוף ציבורי כהגדרתו בסעיף 23;

21. (3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

22. (ב) בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

23. (ג) לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

24. בהתחשב בקביעת הרשות להגנת הפרטיות – הרי שהמשיבה, הפרה את בעיף 17 לחוק, ולא אבטחה את המידע הרגיש של לקוחותיה – דבר שהסב, מסב ויסב נזק כלכלי ואף נזק לא ממוני ללקוחותיה.

25. כאמור דלעיל, הרי שנראה כי המשיבים בחרו להתעלם כמעט לחלוטין, מחובות אבטחת המידע המצוי במאגר המידע.

ב. **הצדדים:**

26. כאמור המשיבה הנה חברת ביטוח בישראל, ולה כמיליון לקוחות בישראל.

27. המבקש הנו מבוטח של המשיבה, אשר קיבל מידיה הודעה בדבר פריצת האבטחה.

- העתק מהודעת המשיבה לידי המבקש מצ"ב **נספח "6"** לבקשה זו.

ג. **רקע עובדתי:**

הפרת הוראות הדין בידי המשיבים:

28. כאמור, המשיבה, הפרה את חובות האבטחה כלפי המבקש, וחברי הקבוצה..

29. בשל האמור, למבקש ולחברי הקבוצה, עומדת עילה אישית כנגד המשיבים ונגרם לו נזק מובהק.

ד. הטיעון המשפטי

(א) בסיסי

30. חוק תובענות ייצוגיות – שנכנס לתוקף לא מזמן במונחי חוק ומשפט – נועד להסדיר באופן ממצה את הדינים החלים על הגשת תביעות ייצוגיות בישראל

31. המטרות שביסוד החוק מפורטות בו בסעיף 1, וכוללות בין השאר את המטרות של ***"אכיפת הדין והרתעה מפני הפרתו"***, ***"מימוש זכות הגישה לבית המשפט"***, ***"מתן סעד הולם לנפגעים מהפרת הדין"*** וכן ***"ניהול יעיל, הוגן וממצה של תביעות"***.

32. חוק התובענות הייצוגיות מתיר הגשת תביעה ייצוגית בעניינים המנויים בתוספת השניה לחוק, או בעניינים בהם נקבע בהוראת חוק מפורשת כי ניתן להגיש תביעה ייצוגית. כאמור בסעיף 3(א) לחוק:

> ***" לא תוגש תובענה ייצוגית אלא בתביעה כמפורט בתוספת השניה או <u>בענין שנקבע בהוראת חוק מפורשת כי ניתן להגיש בו תובענה ייצוגית</u>"***

33. התוספת השניה לחוק התובענות היצוגיות כוללת רשימה של עילות בהן ניתן להגיש תביעה ייצוגית. לענייננו, העילות הקבועות בסעיפים 1-2 לתוספת השניה הן הרלוונטיות:

> ***"תביעה נגד עוסק, כהגדרתו בחוק הגנת הצרכן, בקשר לענין שבינו לבין לקוח, בין אם התקשרו בעסקה ובין אם לאו".***

וכן:

> ***"תביעה נגד מבטח, סוכן ביטוח או חברה מנהלת, בקשר לענין, לרבות חוזה ביטוח או חוזה ביטוח או תקנון קות גמל, שבינהם לבין הלקוח לרבות מבוטח או עמית, בין אם התקשרו בעסקה ובין אם לאו".***

34. סעיף 4 לחוק תובענות ייצוגיות קובע את רשימת הזכאים להגיש בקשה לאישור תובענה ייצוגית. לענייננו רלוונטי סעיף 4 (א)(1) לחוק:

> ***"אדם שיש לו עילה בתביעה או בעניין כאמור בסעיף 3(א), המעוררת שאלות מהותיות של עובדה או משפט המשותפת לכלל החברים הנמנים עם קבוצת בני אדם- בשם אותה קבוצה."***

35. כלומר, על מנת להיות זכאי להגיש בקשה לאישור תביעה ייצוגית, על המבקש להראות כי עומדת לו עילת תביעה באחד העניינים המנויים בתוספת השניה וכן כי התביעה מעוררת שאלות מהותיות של עובדה ומשפט המשותפות לכלל חברי קבוצת התובעים.

36. ולישום לענייננו, על המבקש להראות כי עומדת לו עילת תביעה כנגד המשיבים, וכי עילת התביעה מעוררת שאלות משותפות של עובדה ומשפט לכלל חברי קבוצת התובעים.

37. בשלב של הבקשה לאישור תביעה ייצוגית על המבקש לשכנע את בית המשפט הנכבד כי עומדת לו לכאורה עילת תביעה אישית, אך אין להעמיד בהקשר זה דרישות מחמירות. עמדה על-כך השופטת שטרסברג כהן בע"א 2967/95 **מגן וקשת בע"מ נ' טמפו**, פ"ד נא(2) 312 (פסקה 19 לפסק-דינה):

"נראה לי, כי על המבחן למילוי התנאים שבסעיף 54 מבחינת נטל ומידת ההוכחה, להיות אחיד לכל סעיפיו המשניים, ולגבי כל התנאים הנדרשים מהתובע, ועליו לשכנע את בית המשפט במידת הסבירות הראויה ולא על פי האמור בכתב התביעה בלבד, <u>כי הוא ממלא לכאורה</u> אחר כל דרישות סעיף 54א ולענייננו, שהראשונה בהן היא קיומה של עילה אישית כאמור בס' 54א(א). <u>אין להעמיד דרישות מחמירות מדי, לענין מידת השכנוע, משום שאלה עלולות להטיל על הצדדים ועל בית המשפט עומס יתר בבירור הנושא המקדמי, דבר העלול לגרום להתמשכות המשפט, לכפילות בהתדיינות ולרפיון ידים של תובעים ייצוגיים פוטנציאליים</u>. את כל אלה יש למנוע על ידי קריטריון מאוזן בנושא נטל ומידת ההוכחה הנדרשים מהתובע הייצוגי, שמצד אחד שלא יפטור אותו מחובת שכנוע ומצד שני לא יטיל עליו נטל כבד מדי.

(ההדגשות אינן במקור – י.ג. וט.ר)

38. בנוגע להוכחת הנזק, חוק תובענות ייצוגיות קובע כי די בהוכחת גרימה של נזק ברמה לכאורית. כאמור בסעיף 4(ב)(1) לחוק:

"בבקשה לאישור שהוגשה בידי אדם כאמור בסעיף קטן 1(א) – די בכך שהמבקש יראה כי <u>לכאורה</u> נגרם לו נזק."

(ההדגשות אינן במקור – י.ג. ו ט.ר.)

39. התנאים לאישור תביעה ייצוגית מנויים בסעיף 8(א) לחוק תובענות ייצוגיות, הקובע כי:

8. (א) בית המשפט רשאי לאשר תובענה ייצוגית, אם מצא שהתקיימו כל אלה:

(1) התובענה מעוררת שאלות מהותיות של עובדה או משפט המשותפות לכלל חברי הקבוצה, ויש אפשרות סבירה שהן יוכרעו בתובענה לטובת הקבוצה;

(2) תובענה ייצוגית היא הדרך היעילה וההוגנת להכרעה במחלוקת בנסיבות הענין;

(3) קיים יסוד סביר להניח כי עניינם של כלל חברי הקבוצה ייוצג וינוהל בדרך הולמת; הנתבע לא רשאי לערער או לבקש לערער על החלטה בעניין זה;

(4) קיים יסוד סביר להניח כי עניינם של כלל חברי הקבוצה ייוצג וינוהל בתום לב.

40. בהתאם להוראות שפורטו לעיל, הרי שהדיון משלב זה יחולק לשני שלבים. **בשלב הראשון**, נראה כי עומדת למבקשת עילת תביעה אישית כנגד המשיבים, וכי נגרם לו נזק. **בשלב השני**, נעמוד על התקיימות התנאים לאישור התביעה כייצוגית המנויים בסעיף 8 לחוק תובענות.

(ב) <u>הפרת הוראות חוק הגנת הפרטיות ותקנות אבטחת המידע :</u>

41. נקבע **בע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' אריה ורדי** (23/01/2013 פורסם בנבו) בפסקה 22 לפסק דינו של כבי השופט פוגלמן :

"הזכות לפרטיות היא מהחשובות שבזכויות האדם בישראל. היא אחת החירויות המעצבות את אופיו של המשטר בישראל כמשטר דמוקרטי...ממועד קבלתו של חוק יסוד : כבוד האדם וחירותו, אף מוקנה לה מעמד חוקתי (ס' 7 לחוק היסוד) הפרטיות מאפשרת לאדם לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בהתנהגותו ובמעשיו הפרטיים. היא "מבצרו" הקנייני, האישי והנפשי"... הזכות לפרטיות, אם כן, מותחת את הקו בין הפרט אל הכלל, בין האני לבין החברה. היא משרטטת מתחם אשר בו מניחים את הפרט לנפשו לפיתוח האני שלו. בלא מעורבות של הזולת... היא "מגלמת את האינטרס היחיד שלא להיות מוטרד בצנעת חייו על ידי אחרים"

42. וכפי שפורט לכל אורך בקשה זו, קבעה הרשות להגנת הפרטיות – באופן רשמי, כי המשיבה הפרה את הוראות חוק הגנת הפרטיות, סעיף 17, ותקנות 2, 4, 5 (א), 9 (ב)(2), 10, 11 (S) ו- 14 (א), לתקנות אבטחת המידע בכך שלא שמרה כנדרש על המידע של מליון לקוחותיה, ופגעה בפרטיותם.

(ג) <u>עוולת הרשלנות :</u>

43. סעיפים 35-36 לפקודת הנזיקין קובעים באופן הבא :

רשלנות

"35. עשה אדם מעשה שאדם סביר ונבון לא היה עושה באותן נסיבות או לא עשה מעשה שאדם סביר ונבון היה עושה באותן נסיבות, או שבמשלח-יד פלוני לא השתמש במיומנות, או לא נקט מידת זהירות, שאדם סביר ונבון וכשיר לפעול באותו משלח-יד היה משתמש או נוקט באותן נסיבות - הרי זו התרשלות; ואם התרשל כאמור ביחס לאדם אחר, שלגביו יש לו באותן נסיבות חובה שלא לנהוג כפי שנהג, הרי זו רשלנות, והגורם ברשלנותו נזק לזולתו עושה עוולה.

חובה כלפי כל אדם

36. החובה האמורה בסעיף 35 מוטלת כלפי כל אדם וכלפי בעל כל נכס, כל אימת שאדם סביר צריך היה באותן נסיבות לראות מראש שהם עלולים במהלכם הרגיל של דברים להיפגע ממעשה או ממחדל המפורשים באותו סעיף."

44. עוולת הרשלנות מורכבת משלושה יסודות: קיום חובת זהירות, הפרת חובת הזהירות וגרימה של נזק. ראה ע"א 145/80 **ועקנין נ' המועצה המקומית בית שמש, פ"ד לז 1, 113, 112 (להלן: "עניין וקנין")**.

45. לעניין קיומה של חובת זהירות איש לא יחלוק כי המשיבים חבים בחובת זהירות, הן מושגית והן קונקרטית, כלפי לקוחותיהם. המשיבים חבים בחובת זהירות, מושגית וקונקרטית, גם כלפי המבקשת.

46. בעניין ועקנין, נקבע כי קיומן של חובת זהירות מושגית וקונקרטית נקבעות בהתאם למבחן הצפיות במסגרתו יש לבחון האם אדם סביר מסוגל לצפות את הנזקים שנגרמו. לענייננו, איש לא יחלוק כי ניתן לצפות את האפשרות לגרימת נזקים בלתי ממוניים עקב פגיעה בפרטיותו לבטח הכלכלית, של מי שפרטי כרטיס האשראי שלו, שמו ומספר זהותו - נגנבים.

47. לעניין הפרת חבות הזהירות, הרי שאין כל ספק כי האירועים נשוא תובענה ייצוגית זו הינם פועל יוצא של התרשלותם של המשיבים. בהתאם לפסיקה, מוטלת החובה על מזיק לנקוט באמצעי זהירות סבירים. כפי שנקבע עניין ועקנין (עמ' 131):

"חובתו של המזיק היא לנקוט אמצעי זהירות סבירים, ואחריותו מתגבשת, רק אם לא נקט אמצעים אלה. סבירותם של אמצעי הזהירות נקבעת על-פי אמות מידה אובייקטיביות, המגולמות באמירה, כי על המזיק לנהוג, כפי שאדם סביר היה נוהג בנסיבות העניין. אדם סביר זה אינו אלא בית המשפט, אשר צריך לקבוע את רמת הזהירות הראויה. רמת זהירות זו נקבעת על-פי שיקולים של מדיניות משפטית השאלה אינה, מהו האמצעי שמבחינה פיסית מונע נזק, אלא השאלה היא, מהו האמצעי שיש לדרוש כי ינקטו אותו בנסיבות העניין. על בית המשפט לאזן בין האינטרס של הפרט הניזוק לביטחונו האישי, לבין האינטרס של המזיק לחופש פעולה, וכל זה על רקע האינטרס הציבורי בהמשכה או בהפסקתה של אותה פעילות. על בית המשפט להתחשב בסכנה ובגודלה. עליו להתחשב בחשיבותה החברתית של הפעולה. עליו לשקול את האמצעים הדרושים למניעתה"

48. לענייננו, על המשיבה היה לאבטח את פרטי לקוחותיה, וכל הפרטים שהיא לא שמרה עליהם.

49. אך מובן, כי במבחן התוצאה, הרי שהמשיבה לא אבטחה כראוי את הרשומות אשר במאגר המידע. משכך, פועל יוצא מכך, מובן כי המשיבה לא נקטו באמצעי זהרות זה, ובכך היא התרשלה.

50. ביחס לנזק, למבקש נגרם הן נזק כלכלי, והן נזק בלתי ממוני.

51. לעניין הנזק הממוני, היות והמשיבה מקבלת תמורה כספית מלקוחותיה, בגין השירות אותו היא נותנת, והשירות כולל בין היתר, כפי התחייבויותיה החוזיות, וכפי חובותיה הרגולטוריות, אף לשמור על פרטי לקוחותיה, וכל הפרטים האחרים, הרי שהיא הפרה את ההסכם כלפיה, ונתנה שירות חלקי, ולפיכך, עליה להשיב חלק יחסי מדמי הביטוח אותו היא גבתה מלקוחותיה, וחלק זה הנו 20% מדמי הביטוח שגבתה מכל לקוחותיה מ-7 השנים האחרונות.

52. המבקש – סובר כי לאור האמור, יש לפצותה, בסכום של 500 ₪, המהווה 20% מהסכומים אותם שילם לידי המשיבה.

53. ביחס לנזק שאינו ממוני, הרי שאך מובן, שמרגע שהמשיבה, אחראית בשל התנהלותה, לאי אבטחת המידע של לקוחותיה, הם חברי הקבוצה, , אשר בידיה ובמאגריה, הרי שבהתנהלותה, היא העמידה את המבקש, ועודה מעמידה אותו – בסיכון כלכלי של ממש.

54. בשל העמדת המבקש, וחברי הקבוצה – בסיכון של ממש, וכן פגיעה ליבתית באוטונומיה של לקוחותיה, על המשיבה לפצות את המבקשת ואת חברי הקבוצה, בסכום של 1,000 ₪.

55. סך נזקי המבקש – הנם 1,500 ₪.

<u>(ג) עילת הפרת חובת תום הלב</u>

56. חובת תום הלב מהווה עיקרון חשוב החל על כל פעולה משפטית, וכן על ביצוע חיובים שאינם בגדר חוזה כהגדרתם בסעיף 61(ב) לחוק החוזים. מקום בו גוף כלכלי כדוגמת המשיבה הנותן שירות מכירתי לצרכנים ומכך נוצר לו רווח, הרי שמוטלת עליו נורמת התנהגות שהיא מעבר לחובת תום הלב הבסיסית.

57. **סעיף 12 לחוק החוזים מדבר על תום לב במשא ומתן:**

12. (א) במשא ומתן לקראת כריתתו של חוזה חייב אדם לנהוג בדרך מקובלת ובתום לב.

(ב) צד שלא נהג בדרך מקובלת ולא בתום-לב חייב לצד השני פיצויים בעד הנזק שנגרם לו עקב המשא ומתן או עקב כריתת החוזה, והוראות סעיפים 10, 13 ו-14 לחוק החוזים (תרופות בשל הפרת חוזה), תשל"א-1970, יחולו בשינויים המחוייבים.

58. **סעיף 39 לחוק החוזים מדבר על קיום בתום לב:**

39. בקיום של חיוב הנובע מחוזה יש לנהוג בדרך מקובלת ובתום לב; והוא הדין לגבי השימוש בזכות הנובעת מחוזה.

59. בת"א 2405/04 **בן עמי נ' הדר חברה לביטוח בע"מ** נקבע-

"הטעייה על-פי סעיף 2 לחוק יכול שתהא גם במחדל, כאשר גילויו של ענין מהותי לצרכן מתבקש בנסיבות הענין [...] החזקה היא כי הצרכן נותן אמון בעוסק; לא ניתן להטיל על הצרכן את הנטל לברר האם המוצר שרכש עונה על דרישות החוק או התקן".

(ההדגשות אינן במקור - י.ג וט.ר)

60. יצויין, כי ממהות ונסיבות עיסוקה של המשיבה והעובדה כי המשיבה עוסקת במתן שירות ו/או מכר לציבור גדול, יש להחיל עליה גם את עקרון "הדואליות הנורמטיבית" המחיל את עיקר כללי המשפט המנהלי, לרבות חובת תום לב מוגברת, חובת הגינות וכיוצ"ב (ר' ע"א 3414/93 **שמחה און נ' מפעלי בורסת היהלומים**, פורסם בנבו, 29.11.1995, פסקה 6):

"..לאחרונה עשתה הדואליות הנורמאטיבית צעד נוסף, גדול וחשוב. היא פרצה מן התחום של המינהל הציבורי אל התחום של המגזר הפרטי. בית המשפט פסק שהיא עשויה לחול גם על גוף פרטי, שלא הוקם על-ידי חוק, אין לו סמכויות מכוח חוק ואין הוא משתייך, להלכה או למעשה, למינהל הציבורי...".

(ההדגשות אינן במקור - י.ג וט.ר)

61. מכל מקום, נראה כי המשיבה הפרה את סעיף 21.1 לתנאים הכללים של הסכם ההתקשרות שלה עם מנוייה, עת היא לא שמרה על כל הפרטים שלהם.

(ו) עילת התעשרות שלא כדין:

62. אין ולא יכול להיות כל ספק, כי עומדת למבקש כנגד המשיבה עילת תביעה נוספת מכוח חוק עשיית עושר ולא במשפט, הואיל והמשיבה התעשרה על חשבון המבקש ויתר חברי הקבוצה שלא כדין.

63. בהקשר זה, סעיף 1 **לחוק עשיית עושר ולא במשפט**, תשל"ט-1979 (להלן: **"חוק עשיית עושר"**) קובע כדלהלן:

"(א) מי שקיבל שלא על פי זכות שבדין נכס, שירות או טובת הנאה אחרת (להלן -הזוכה) שבאו לו מאדם אחר (להלן - המזכה), חייב להשיב למזכה את הזכייה, ואם השבה בעין בלתי אפשרית או בלתי סבירה - לשלם לו את שוויה."

64. הנה אם כן, חוק עשיית עושר קובע את העיקרון הבסיסי של חובת ההשבה, אשר נועד למנוע התעשרות שלא כדין של אדם על חשבון רעהו.

65. ודוק, חוק עשיית עושר איננו קובע רשימה סגורה של מצבים בהם נתונה הזכות להשבה, וכדבריו של כב' השופט, כתוארו אז, א' ברק בד"נ 20/82 **אדרס חומרי בנין בע"מ נ' הרלו אנד ג'ונס ג.מ.ב.ה**, פ"ד מב(1) 221, בעמ' 273:

> **"הקטגוריות של עשיית עושר ולא במשפט לעולם אינן סגורות ולעולם אינן שוקטות על השמרים... על השופט לפרש את הוראת המחוקק על פי תכלית החקיקה. התכלית היא, בין השאר, מניעת התעשרות שלא כדין... ביסוד תכלית זו עומדת התפיסה... לפיה יש להורות על השבה מקום שתחושת המצפון והיושר (ex aequo et bono) מחייבת השבה"**

66. כך גם הבהירה כב' השופטת נתניהו בע"א 442/85 **משה זוהר ושות' נ' מעבדות טרבנול (ישראל) בע"מ**, פ"ד מד(3) 661, בעמ' 669:

> **"היתרון בכלי שנותן בידינו החוק הוא בגמישותו... אנו חופשיים להעניק את הסעד בכל מקרה ראוי שבו ההתעשרות מקוממת את חוש הצדק וההגינות והיא עונה בכך על היסוד 'שלא על פי זכות שבדין' שבסעיף 1(א) לחוק".**

67. היסודות שיש להוכיח בעילה של עשיית עושר ולא במשפט, על פי סעיף 1 לחוק עשיית עושר הינם שלושה, כמפורט להלן:

(א) קבלה של נכס, שירות או טובת הנאה אחרת על ידי הזוכה (התעשרות).
(ב) ההתעשרות באה לזוכה מן המזכה או על חשבון המזכה (קשר סיבתי).
(ג) התעשרות הזוכה נעשתה "שלא על פי זכות שבדין" (יסוד נורמטיבי).
[לעניין זה ראה: ד"נ 20/82 הנ"ל, בעמ' 275, שם]

68. לענייננו, המשיבה עושה עושר כתוצאה מפעילותיה, בכך שהיא יוצרת אי וודאות ביחס לטיב מוצריה, ובכך יוצרת הטעייה והטיה של התנהלות צרכנית, ואין כל ספק שתוספת העושר כולה היא על גבם ועל חשבונם של חברי הקבוצה המיוצגת, עת היא נמנעה מלשהשקיע כספים באבטחת המידע של לקוחותיה. ולפיכך, מחובתה להשיב לידי לקוחותיה את הסכום שאבטחת המידע הייתה עולה, לא הייתה מבצעת היא את כל הנדרש לשם שמירת פרטיותם של לקוחותיה.

69. האמור נכון אלפי מונים - אף ביחס למשיבה כחברת ביטוח.

70. כאמור המשיבה גורמת ללקוחותיה, לשלם עבור מוצר תקין וזאת ללא יידועם כי היא לא שומרת על פרטיות לקוחותיה, ופועלת לפי האינטרסים הכלכליים שלה.

ה. התקיימות התנאים לאישור התביעה כייצוגית

71. להלן נעמוד על התקיימות התנאים הקבועים בסעיף 8(א) לחוק התבוענות הייצוגיות כסדרם.

<u>פרטים הנוגעים לקבוצה</u>

72. יובהר ראשית, תפקידו של בית המשפט הנכבד הוא להגדיר את קבוצת התובעים, כאמור בסעיף 10(א) לחוק התובענות הייצוגיות בו מצויין כי "אישר בית המשפט תובענה ייצוגית, יגדיר בהחלטתו את הקבוצה שבשמה תנוהל התובענה".

73. המבקש יטען כי מן הראוי שהקבוצה תכלול " כל אדם או אישיות משפטית אחרת, אשר הפרטים שלהם נכללו במאגר המידע של שירביט, ונחשפו, כתוצאה מהארועים הקשורים בדיווח של רשויות הביטוח והסייבר ו/או כל המבוטחים אשר הפרטים שלהם כלולים במאגר המידע של שירביט ואשר סבלו ו/או יסבלו מעוגמת נפש כתוצא מפרסום דבר פרשת דליפת המידע ו/או כל המבוטחים אשר הפרטים האישיים שלהם נכללו במאגר המידע של שירביט, והמידע השמור נפגם כולו או חלקו"".

74. מראש יצויין כי אין זה מחובתו של המבקש להעריך במדויק את גודל הקבוצה ואת סכום הפיצוי המבוקש לכלל חברי הקבוצה, דבר שניתן יהיה לגלות במדויק רק לאחר חשיפת הנתונים ע"י המשיבה. ברי, כי אין למבקש כל יכולת לדעת את כמות האנשים שנפגעים בענייננו זה.

75. חזקה על המשיבה, המוכרת ברבים כחברת ביטוח גדולה, כי כל נתון רלוונטי שמור במאגרי הנתונים שלה באופן שיטתי ומסודר, המאפשר את דלייתו בנקל.

76. במהלך הליך זה, יעתור, איפוא, המבקש לחיובה של המשיבה בחשיפת כל הנתונים הרלוונטיים ובכלל זאת מספר הלקוחות ונתוניהם האישיים.

77. המבקשת מעריך כי מספרם של חברי הקבוצה הנו כמיליון לקוחות.

78. ברור כי אין המדובר במקרה יחידני והמשיבים פועלת באופן שיטתי וגורף וכי קיימת קבוצה שלמה של תובעים אשר כלל אינם ידעו ו/או יודעים כי הם נתוניהם לרבות מספר כרטיס האשראי שלהם, נגנבו, בשל מחדלי המשיבה.

79. המבקש מעריך **<u>בשמרנות מירבית</u>** כי מדובר במיליון לקוחות שנפגעו מפגיעה בפרטיותם, ונזקם מוערך בסך של כ 2,000 ₪ לאדם .

80. באופן שמרני מעמיד המבקש את תביעתו האישית על סך 1,500 ₪ לעניין הנזק (בפועל) והנזק הלא ממוני (עוגמת נפש, ופגיעה ליבתית באוטונומיה), כאשר לגבי חברי הקבוצה, בהערכה שמרנית ועל דרך האומדנא, יטען המבקש כי סך של 1,500 ₪ ללקוח הוא הסעד הראוי אותו יש לפסוק גם ליתר חברי

הקבוצה. בהנחה כי מדובר ב- מליון חברי קבוצה, ובגדרי התקופה הרלוונטית, הרי שסכום התביעה הכולל עומד על סכום מאד גבוה.

81. למרות האמור, יעמיד התובע את תביעת הקבוצה, ע"ס 600,000,000 ₪ - וזאת על דרך הזהירות.

82. כידוע, השאלה העיקרית הניצבת על הפרק בשעה שבוחנים האם "גודל הקבוצה" מצדיק הכרה בתובענה כייצוגית הנה האם יהיה זה בלתי מעשי לצרף לתביעה "רגילה", כתובעים את כל חברי הקבוצה (ראה גם ג' לוטן ו-א' ארז, תובענות ייצוגיות (כרך א'), (הוצאת תמר התשנ"ו), עמ' 154 והאסמכתאות הנזכרות שם). כמובן, שצירופם של כל חברי הקבוצה לתביעה "רגילה" אינו מעשי.

83. בנסיבות אלה, ובשים לב לכך שנזקיו האישיים של כל חבר וחבר בקבוצה הנם נמוכים יחסית (עניין שיידון בהמשך), יהיה זה בלתי מעשי לצפות מחברי הקבוצה לנהל באופן עצמאי הליכים משפטיים נפרדים, כל חבר ועניינו הוא נגד המשיבה המוכרת וידועה בישראל. זאת ועוד, לא יהיה מעשי לצרף את כל חברי הקבוצה כתובעים משותפים בתביעה אחת, שאינה ייצוגית, וזאת בשל סיבות רבות, בין היתר:

א. שמות חברי הקבוצה שמורים אך ורק בידי המשיבה– והיא לא תתנדב למסור לתובע את שמותיהם.

ב. כל שאר הנתונים – מצויים בידי המשיבים ובלבד – נתונים שספק אם המשיבים יסכימו לחשוף – כך סתם, ואולם חזקה עליה, כי לאחר שתצווה להציגם, כמקווה, היא תעשה כן במתכונת ובמועד שיקבעו לשם כך.

ג. צפיפות וחוסר יכולת מעשית לנהל משפט בו יטלו חלק עשרות אלפי בעלי דין.

84. אמור מעתה: גודלה של הקבוצה, על כל הנגזר ממנו, מצדיק הכרה בתובענה כתובענה ייצוגית.

<u>שאלות זהות של עובדה ומשפט</u>

85. התובענה **מעוררת** שאלות זהות של עובדה ומשפט המשותפות לכל חברי הקבוצה ומצדיקות הגשת תובענה על דרך תובענה ייצוגית, שכן, ההפרה זהה אצל כל חברי הקבוצה. משמע:

(א) עילות התביעה הינן זהות לגבי כל אחד מחברי הקבוצה.

(ב) הנזק זהה.

86. יוצא, איפוא, כי כמובן התשובות לשאלות המשפטיות שהוצבו לעיל, משותפות לכל חברי הקבוצה, וההכרעה בה בגדרה של תובענה ייצוגית, תייתר הצורך בניהולם של אלפי הליכים נפרדים, ותסייע לבית המשפט הנכבד ולכלל הציבור בערכים של יעילות ועשיית צדק.

<u>הדרך היעילה וההוגנת</u>

87. ניהול התובענה דנן כייצוגית הינו ללא ספק הדרך היעילה וההוגנת לניהול הליך.

88. בהקשר זה, מן הראוי לחזור ולציין המטרות שביסוד חוק תובענות ייצוגיות, המפורטות בו בסעיף 1, וכוללות בין השאר את המטרות של "***אכיפת הדין והרתעה מפני הפרתו***", "***מימוש זכות הגישה לבית המשפט***", "***מתן סעד הולם לנפגעים מהפרת הדין***" וכן "***ניהול יעיל, הוגן וממצה של תביעות***".

89. לענייננו, יש באישור התביעה הייצוגית כדי להגשים את המטרות שצוינו לעיל בכללותן.

90. ראשית, יש בהגשת תביעה ייצוגית זו בכדי לתרום משמעותית להרתעה של המשיבים – ומעוולים כדוגמתה – מלפגוע בצורה חמורה בציבור במקרים כדוגמת המקרה נשוא תובענה זו.

91. שנית, תובענה זו היא הכרחית על מנת לממש את זכאותם לפיצוי של חברי הקבוצה כלפי המשיבים.

92. בסכום התביעה האישי הנמוך, העומד לתובע פוטנציאלי, אין די על מנת לתמרץ תובע לפתוח בהליך משפטי מורכב ומסובך כנגד גופים עוצמתיים במיוחד כדוגמת המשיבים, וראה בהקשר זה את הדברים שנאמרו ברע"א 4556/94 **טצת ואח' נג' זילברשץ ואח'**, פ"ד מט (5) 774, בעמ' 784.

93. סביר להניח, אפוא, וזהו השיקול העיקרי, כי לחברי הקבוצה – רובם ככולם – אין מוטיבציה לקיים הליך משפטי ממושך ומייגע כנגד המשיבים בתקווה לזכות בסיומו לסכום הקטן. לפיכך הדרך היחידה להגן על אלה הנה הדרך של התובענה הייצוגית.
(ראו רע"א 4556/94 **טצת ואח' נג' זילברשץ ואח'**, פ"ד מט (5) 774, בעמ' 784 מול האות ב').

94. עוד יש להוסיף כי הכרעה אחת בתובענה ייצוגית תמנע את הסיכון של פסיקות סותרות ע"י בתי-משפט שונים, אשר עשויים לדון באותו נושא ממש.

95. זאת ועוד; בחירה במסלול דיון, שיאפשר התדיינות אחת חלף התדיינויות רבות, תביא לחסכון בזמן שיפוטי יקר, אשר ממילא חסר הוא למערכת בתי המשפט, אשר דומה, כי בימים אלה נאבקת תחת עומס כבד – שיקול מערכתי שיש ליתן לו משקל מוגבר.

ייצוג הולם ודרישת תום הלב.

96. התובענה שבנדון הוגשה בתום לב ובנקיון כפיים על ידי המבקש שהינו לקוח של המשיבה לפני שנודעו לו פרטי הנסיבות והפרטים שהביאו אותו לשאת את ה"עול" האומץ והאחריות הציבורית להיות "תובעי ייצוגי" על כל המשקל הרב הנובע מכך.

97. לעניין הייצוג ההולם, הרי שהמבקש הינו בעל אמצעים כלכליים הנדרשים לשם ניהול ההליך. המבקש ייוצג על ידי עוה"ד הח"מ, המבטיח להעמיד לרשות הקבוצה ייצוג משפטי ככל שיידרש על מנת לממש את זכויות החברים בקבוצה כלפי המשיב.

כמו כן, ראוי להדגיש, כי הח"מ, הינם עו"ד עתיר ניסיון בתחום התובענות הייצוגיות ככלל וכן מנהל זה מכבר מספר תביעות ייצוגיות רבות.

צו עשה וסעד הצהרתי:

98. בית המשפט הנכבד מתבקש בזאת ליתן צו הצהרתי לפיו המשיבים הפרו את הוראות הדין, כמו כן, מתבקש ביהמ"ש הנכבד ליתון צווי עשה, ולהורות למשיבה לפעול ולאבטח את מאגר המידע של המשיבה, שבו מצויים פרטי חברי הקבוצה ונכסים שלהם, לרבות רכבים, הן כלפיי סיכוני חוץ והן כלפי סיכוני פנים הארגון.

ז. סיכום

99. מכל האמור לעיל מתבקש בית המשפט הנכבד:

(א) לאשר למבקש לנהל תובענה כייצוגית בשמם של חברי הקבוצה, בהתאם להגדרתה לעיל.

(ב) להצהיר כי המשיבים אינה מקיימת את הוראות החוק, ולהוציא צו המורה למשיבים לקיימן לאלתר וכפי שפורט בצו העשה שלעיל.

(ג) להורות למשיבים לפצות את לקוחותיה הנמנים על חברי הקבוצה בסך כולל של **600,000,000 ₪** .

(ד) להורות על פסיקת פיצוי מיוחד למבקש.

(ה) להורות על תשלום שכר טרחת עורך-דין לעורכי הדין המייצג באחוזים מתוך הקרן בהתאם לשיקול דעתו של בית המשפט הנכבד וכן על תשלום הוצאות משפט.

יוחי גבע, עו"ד

ב"כ המבקש

תצהיר

אני הח"מ יהודה חכם נושא ת"ז מס' 51884955 לאחר שהוזהרתי כי עליי להצהיר את האמת אחרת אהיה צפויה לעונשים הקבועים בחוק באם לא אעשה כן מצהירה בזה כדלקמן.

1. המשיבה הנה חברה ביטוח, ולה כ- 1,000,000 לקוחות.

2. ביום 1.12.20, הודיע רשות שוק ההון, ביטוח וחיסכון ומערך הסייבר הלאומי, שהאקרים פרצו לאתר ולשרתי המשיבה.

   העתק מהודעת מערך הסייבר הלאומי, מצ"ב ומסומן: "3".

3. כתוצאה מן הפריצה, הועברו פרטים רבים של לקוחות המשיבה, לידי ההאקרים, ורבים מהם, אף פורסמו ברשת.

4. כל למשל פורסמו, רשיונות נהיגה, תעודות זהות, תביעות ביטוח, תלושי שכר, קרנות השתלמות קרנות פנסיה, ועוד פרטים רבים ביותר של לקוחות החברה.

5. ההאקרים מקבוצת BlackShadow, שפרצו לשרתי המשיבה, אמרולעיתונאים בישראל, כי ברשותם יש טרות (אלפי ג'יגה-בייט) של מידע, וכי בכוונתם למכור את פרטי הלקוחות שדלפו. במסמכים שדלפו, נראים בין היתר גם כמה מסמכים על היעדר עבר ביטוחי הכוללים שמות מלאים, כתובות, ותעודות זהות.

6. הדלפת המסמכים נמשכה אף בלילה שלאחר מכן.
   קבוצת ההאקרים קיבלה אחריות על הפריצה לשרתי החברה, ופרסמה בחשבונות הטוויטר והטלגרם שלה פרטי לקוחות ומסמכים בהיקף עצום, משנת 2012 ועד שנת 2020. תחילה הנפח של אותם פרטים נאמד ב-929 ג'יגה-בייט, אך לדבריהם מדובר באלפים. על פי הערכות, מדובר במידע של מאות אלפי מבוטחים, ולעיתים הוא כולל מספרי תעודות זהות - המשמשים בגופים רבים, גם ממשלתיים, כאמצעי אימות משני. לפני פחות מחודש זכתה שירביט במכרז לביטוח רכב פרטי לעובדי מדינה בשנת 2021, ומבוטחים בה רבים המשרתים בכוחות הביטחון.

   בין ההקלטות שפורסמו בעמוד הטלגרם של התוקפים, ישנה שיחה עם לקוחה, מספר תעודת הזהות שלה ופרטי התאונה שעליה דיברה עם החברה. בנוסף, פורסם מייל ובו פרטי כרטיס אשראי.

   צילום מקצת החומרים האישיים שהודלפו לרשת (לרבות של כבוד השופט גלעד נוייטל), מצ"ב ומסומן: "4".

7. לתדהמת לקוחות המשיבה, הוברר בתקופה האחרונה, כי המשיבה הפרה את חוק הגנת הפרטיות, תקנות הגנת הפרטיות את ההסכמים עם לקוחותיה, וחובות נוספים, בכך, שבשל התרשלותה, והפרת חובותיה, עת היא לא שמרה על פרטי לקוחותיה, ואלו היום חשופים לכל, פשוטו כמשמעותו.

8. למעשה, בשל פירצת האבטחה המורה ביותר שניתן לדמיין, וחולשות האבטחה החמורות שהוברר שקיימות במערכות ובשרתי המשיבה, כמו גם, בשל בשל רשלנותה של המשיבה, הרי שכל המידע האישי של הלקוחות, בשמם המלא, כתובתם, מספרי הטלפון שלהם, מספרי הזהות שלהם, מספרי חשבונות הבנק שלהם, ספרות אחרונות בכרטיסי האשראי של הלקוחות, ועוד מידע רב - נחשף, והכל כפי שהיה מצוי בבמאגר המידע של המשיבה.

9. בהתאם לאמור, מובן שהמשיבה, לא טיפלה בהתאם לחובתה, בנושאי אבטחת המידע, הנוגעים לפרטי לקוחותיה, לרבות כל המידע דלעיל, ולמעשה הפקירה את פרטיות לקוחותיה.

10. בשל כך, תרמה המשיבה לחשיפת מידע בהיקף רחב ביותר, וברמות רגישות גבוהות, תוך שהיא התעלמה מסיכון זליגת המידע, מתוך החברה ומחוצה לה, וביצוע השימוש במידע, מעבר למטרות שלשמן נשמר המידע.

11. זאת ועוד, המשיבה פרסמה הודעה ללקוחותיה, אשר מלמדת כי היא איננה מבינה את עוצמת הנזק שנגרם ללקוחותיה.

12. בכך הפרה המשיבה, את חובותיה, האמורים בסעיף 17 לחוק הגנת הפרטיות, התשמ״א – 1981, ובכך העמידה בסיכון ממשי, את מליון לקוחותיה.

13. בנוסף, הפרה המשיבה את תקנות 2, 4, 5 (א), 9 (ב)(2), 10, 11 (S) ו- 14 (א), לתקנות אבטחת המידע.

14. זאת ועוד, ביום 31.8.16, פרסמה הממונה על שוק ההון ביטוח וחיסכון, הגב׳ סלינגר, חוזר לגופים מוסדיים 2016-9-14, תחת הכותרת ״ניהול סיכוני סייבר בגופים מוסדיים״.

העתק החוזר, מצ״ב ומסומן: ״5״.

15. הוראות החוזר, אינן משתמעות לשתי פנים.

16. המשיבה הפרה אף את הוראות החוזר.

17. כתוצא ממחדלי המשיבה, הרי שפרטי לקוחותיה, לרבות המידע האישי של הלקוחות, שמם המלא, כתובתם, מספרי הטלפון שלהם, מספרי הזהות שלהם, מספרי לוחיות הרכב שלהם, מספרי שלדות

הרכב שלהם, חשבוניות הלקוחות, מספרי חשבונות הבנק שלהם, ספרות אחרונות בכרטיסי האשראי של הלקוחות, היו פרוצים לכל, והכל כפי שהיה מצוי בבמאגר המידע של המשיבה.

18. אך מובן, כי כתוצאה מההפרה, נגרמו לחברי הקבוצה, נזקי, הן ממוניים והן בלתי ממוניים, לרבות העמדה בסיכון ממשי – לרבות נזק כלכלי.

19. עוד מובן, כי המשיבה הפרה את הוראות הדין כמו גם הוראות חוק חוזה ביטוח, תקנות הביטוח שלפי החוק, והוראות הרגלוטור ביחס לחובותיה כלפי לקוחותיה כמבטחת.

20. עוד הפרה המשיבה, את ההסכמים כלפי לקוחותיה, עת נכשלה בכישלון חרוץ, בשמירה על המידע האישי של לקוחותיה, ואשר נמסר לה על ידיהם.

21. התנהגות המשיבה, איננו מתקבל על הדעת, ומהווה פגיעה חמורה בפרטיות של חברי הקבוצה.

22. עוד מהווה התנהגותה, הטעיה והתרשלות, הפרת חובה חקוקה והפרת הסכם כלפי חברי הקבוצה.

23. בנסיבות אלו, אין מנוס מהגשת תובענה ייצוגית מוצדקת זאת, על מנת לזכות את חברי הקבוצה בפיצוי המגיע להם, בשל הפגיעה בפרטיותם, וכן בשל ההטעיה וההתרשלות כלפיהם.

24. חוק תובענות ייצוגיות, עוד בסעיף 1 לחוק, מגדיר כי הוא נועד :
"לשם שיפור ההגנה על זכויות".

1. זכות בסיסית מרכזית, הטעונה שיפור ובאופן דחוף, היא זכותו של האדם בכלל, ולקוחותיהם של המשיבה בפרט, **לפרטיות**. מדובר בזכות חוקתית כחלק מזכותו של האדם לכבודו. כפי שנקבע בע"פ **5026/97 גלעם ואח' נ' מדינת ישראל**, דינים עליון נו 164 :

"הנה כי כן : הזכות לפרטיות היא, בין היתר, אחת הנגזרות של הזכות לכבוד. הכרה בפרטיות היא ההכרה באדם כפרט אוטונומי הזכאי לייחוד אל מול האחרים. ייחוד זה הוא המאפשר לאדם להתבצר באישיותו כבעלת משמעות הראויה לכיבוד. פרטיותו של אדם היא כבודו וגם קניינו. זוהי המסגרת באמצעותה הוא עשוי ם הוא בוחר בכך. לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בתנהגותו ובמעשיו הפרטיים. זהו "מבצרו" הקנייני, האישי והנפשי".

2. זכות זו נרמסת באופן גס בידי המשיבה, להבדיל ממתחריה בשוק, בניגוד מוחלט להוראות הדין ולהוראות הרגולטור, אשר לדאבון הלב אינן נאכפות.

3. **עסקינן, כאמור, בהתרשלות רבתית, באבטחת מידע רגיש ביותר, של הלקוחות, דבר אשר חשף את פרטיהם האישיים.**

4. לאור נסיבות התנהלות המשיבות כאמור לעיל ולהלן, נטען כי למעשה קשה לחשוב על מקרה מובהק יותר, המצדיק הגשת תובענה ייצוגית. על המשיביה יהיה לפצות את לקוחותיהם אשר פרטיותם נפגעה. כן יתבקשו צווים שתכליתם למנוע את המשך הפרת הוראות הדין. על כל להלן.

__א.2. על הזכות לפרטיות__

5. הזכות לפרטיות בע"פ **5026/97 גלעם ואח' נ' מדינת ישראל**, דינים עליון נו 164:

"הנה כי כן: הזכות לפרטיות היא, בין היתר, אחת הנגזרות של הזכות לכבוד. הכרה בפרטיות היא ההכרה באדם כפרט אוטונומי הזכאי לייחוד אל מול האחרים. ייחוד זה הוא המאפשר לאדם להתבצר באישיותו כבעלת משמעות הראויה לכיבוד. פרטיותו של אדם היא כבודו וגם קניינו. זוהי המסגרת באמצעותה הוא עשוי ס הוא בוחר בכך. לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בתנהגותו ובמעשיו הפרטיים. זהו "מבצרו" הקנייני, האישי והנפשי".

6. וכך גם נקבע **בע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' אריה ורדי** (23/01/2013 פורסם בנבו) בפסקה 22 לפסק דינו של כב' השופט פוגלמן:

"הזכות לפרטיות היא מהחשובות שבזכויות האדם בישראל. היא אחת החירויות המעצבות את אופיו של ההמשטר בישראל כמשטר דמוקרטי...ממועד קבלתו של חוק יסוד: כבוד האדם וחירותו, אף מוקנה לה מעמד חוקתי (ס' 7 לחוק היסוד) הפרטיות מאפשרת לאדם לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בהתנהגותו ובמעשיו הפרטיים. היא "מבצרו" הקנייני, האישי והנפשי"... הזכות לפרטיות, אם כן, מותחת את הקו בין הפרט אל הכלל, בין האני לבין החברה. היא משרטטת מתחם אשר בו מניחים את הפרט לנפשו לפיתוח האני שלו. בלא מעורבות של הזולת... היא "מגלמת את האינטרס היחיד שלא להיות מוטרד בצנעת חייו על ידי אחרים"

ראה בנוסף **רעא 4447/07 רמי מור נ' ברק אי טי סי(1995) החברה לשרותי בזק בינלאומיים בע"מ** (25/03/2010, פורסם בנבו) פסקה 13 לפסק דינו של המשנה לנשיא ריבלין:

7. הזכות לפרטיות אינה מתמצה בזכוותו של האדם לנהל את חייו בביתו שלו ללא חדירה לפרטיותו, ויש להבינה ולעבדה באופן רחב יותר. כזכותו של האדם "להעזב לנפשו". יפים בהקשר זה דבריו של השופט גרוניס בבג"צ **8070/90 האגודה לזכויות האזרח בישראל נ' משרד הפנים ואח'** בפסקה 2:

ישתי פנים לה לזכות הפרטיות הנזכרת בסעיף 7א לחוק יסוד כבוד האדם וחירותו. הפן האחד שניתן למצוא מקרי בכבוד האדם, הינו "זכותו של אדם לנהל את אורח החיים שבו הוא חפץ בדל"ת אמות ביתו, בלא הפרעה מבחוץ" (בג"צ 2481/93 דיין נ' ניצב יהודה וילק, פ"ד מח(2) 456, 470 וכן ראו ע"פ 1302/92 מדינת ישראל נ' נחמיאס, פ"ד מט2 309,353) ***__אין להוביל אמירה זו להביט הפיזי של הבית. יש להבינה בצורה רחבה יותר, באופן מטפורי ברוח הביטוי שטבעו וורן__***

<u>וברנדייס "the right to be left alone" (s.d warren & l.d brandies "the right to privacy" 4 harv. L. rev 193 (1980)."</u>

8. נעלה מכל ספק, כי הזכות לפרטיות ראויה להגנה, הגנה חוקתית, והן הגנה במסגרת אכיפת הוראותיו של חוק הגנת הפרטיות. מיותר לציין, כי כלי התובענה הייצוגית הנועד לשם שיפור ההגנה על זכויות כמו גם אכיפת הוראות הדין הינו המתאים גם לשם שיפור תמונת המצב העגומה בניפי המשיבים – כפי שתפורט להלן.

9. דומה כי קשה לחשוב על מקרה מובהק יותר של פגיעה בפרטיות, מאשר גניבת מידע כלכלי – אישי פרטי של אדם, מקום בו, המשיבה מחזיקה במאגר מידע, המכיל, פרטיו האישיים של אדם, מספר כרטיס האשראי שלו ועוד.

10. לא יתכן, כי חברה, העושה שימוש, בפרטי נכסים של אדם, לרבות רכבו, כרטיסי אשראי, בהם יכול אדם לרכוש מהונו האישי, וחשבון הבנק שלו, והכל באמצעות מספר כרטיס האשראי ופרטים נוספים (לרבות מספר זהות, שם ועוד), תתרשל כלפי אותו אדם, ולא תאבטח באופן מוחלט, ובהתאם לדרישות ממנה – את אותם פרטים – המצויים באותו מאגר מידע.

<u>יצירת מאגר מידע</u>

11. מעבר לפגיעה בפרטיות , הרי שסעיף 7 לחוק הגנת הפרטיות מגדיר המונחים "מאגר מידע" ו- "מידע רגישי" באופן הבא:

*"**מאגר מידע**" - אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט–*

(1) אוסף לשימוש אישי שאינו למטרות עסק; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

מיום 11.4.1996 תיקון מס׳ 4

ס"ח תשנ"ו מס׳ 1589 מיום 11.4.1996 עמ׳ 290 (ה"ח 2234)

*"**מאגר מידע**" – מרכז להחסנת מידע באמצעות מערכת עיבוד נתונים אוטומטית אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט -*

(1) אוסף לשימוש אישי שאינו למטרות עסק; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף;

"מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו;

*"**מידע רגיש**" –*

(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

(2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש;

12. לענייננו, לא תיתכן מחלוקת כי המשיבים יוצרים מאגר מידע של ממש, ובו מידע רגיש כפי שקובעות הנחיות הרשות להגנת הפרטיות החל מסעיף 2.7 ואילך:

7.2 "לפי הגדרות המונחים" מידע "ו"מאגר מידע "בסעיף 7 לחוק ,התחולה של פרק ב 'בחוק היא על שמירת נתונים על אודות אדם ,כאשר המידע אודותיו מזוהה או ניתן לזיהוי. לנוכח מאפייניהן המפורטים לעיל ,חלק ניכר מן ההקלטות ממצלמות המעקב הקיימות כיום נכנס לגדר" מאגר מידע "המתייחס למידע מזוהה ,או ניתן לזיהוי ,אודות אדם, כמשמעותו בסעיף 7 לחוק .בין אלה כלולות:

13. מסקנות הדברים, שוב נזכיר, היא כי שימוש במצמות המעקב גורם ליצירת מאגר מידע, כמשמעותו בהוראות סעיף 7 לחוק הגנת הפרטיות. בענייננו – מדובר אף במדיע רגיש. 3

14. אך מובן, כי המשיבה אוחזת במאגר מידע, הכולל פרטי כרטיסי האשראי, שם ומספר תעודת זהות של לקוחותיה, ופרטים רבים נוספים.

<u>פגיעה בפרטיות:</u>

15. סעיף 17 לחוק הגנת הפרטיות מורה כך:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

16. 17א. (א) מחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר.

17. (ב) מחזיק שברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ימסור לרשם, מדי שנה, רשימה של מאגרי המידע שברשותו, בציון שמות בעלי המאגרים, תצהיר על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על האבטחה כאמור בסעיף 17ב.

18. 17ב. (א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - הממונה):

19. (1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

20. (2) גוף ציבורי כהגדרתו בסעיף 23;

21. (3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

22. (ב) בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף קטן (א).

23. (ג) לא ימונה כממונה מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק זה.

24. בהתחשב בקביעת הרשות להגנת הפרטיות – הרי שהמשיבה, הפרה את בעיף 17 לחוק, ולא אבטחה את המידע הרגיש של לקוחותיה – דבר שהסב, מסב ויסב נזק כלכלי ואף נזק לא ממוני ללקוחותיה.

25. כאמור דלעיל, הרי שנראה כי המשיבים בחרו להתעלם כמעט לחלוטין, מחובות אבטחת המידע המצוי במאגר המידע.

א. <u>הצדדים</u>:

26. כאמור המשיבה הנה חברת ביטוח בישראל, ולה כמיליון לקוחות בישראל.

27. המבקש הנו מבוטח של המשיבה, אשר קיבל מידיה הודעה בדבר פריצת האבטחה.

- העתק מהודעת המשיבה לידי המבקש מצ"ב **<u>כנספח "6"</u>** לבקשה זו.

ב. <u>רקע עובדתי</u>:

<u>הפרת הוראות הדין בידי המשיבים</u>:

28. כאמור, המשיבה, הפרה את חובות האבטחה כללפי המבקש, ותברי הקבוצה..

29. בשל האמור, למבקש ולחברי הקבוצה, עומדת עילה אישית כנגד המשיבים ונגרם לו נזק מובהק.

<u>ד. הטיעון המשפטי</u>

(א) <u>בסיסי</u>

30. חוק תובענות ייצוגיות – שנכנס לתוקף לא מזמן במונחי חוק ומשפט – נועד להסדיר באופן ממצה את הדינים החלים על הגשת תביעות ייצוגיות בישראל

31. המטרות שביסוד החוק מפורטות בו בסעיף 1, וכוללות בין השאר את המטרות של ***"אכיפת הדין והרתעה מפני הפרתו"***, ***"מימוש זכות הגישה לבית המשפט"***, ***"מתן סעד הולם לנפגעים מהפרת הדין"*** וכן ***"ניהול יעיל, הוגן וממצה של תביעות"***.

32. חוק התובענות הייצוגיות מתיר הגשת תביעה ייצוגית בעניינים המנויים בתוספת השניה לחוק, או בעניינים בהם נקבע בהוראת חוק מפורשת כי ניתן להגיש תביעה ייצוגית. כאמור בסעיף 3(א) לחוק:

> ***" לא תוגש תובענה ייצוגית אלא בתביעה כמפורט בתוספת השניה או <u>בענין שנקבע בהוראת חוק מפורשת כי ניתן להגיש בו תובענה ייצוגית</u>"***

33. התוספת השניה לחוק התובענות היצוגיות כוללת רשימה של עילות בהן ניתן להגיש תביעה ייצוגית. לענייננו, העילות הקבועות בסעיפים 1-2 לתוספת השניה הן הרלוונטיות:

> ***"תביעה נגד עוסק, כהגדרתו בחוק הגנת הצרכן, בקשר לענין שבינו לבין לקוח, בין אם התקשרו בעסקה ובין אם לאו".***

וכן:

> ***"תביעה נגד מבטח, סוכן ביטוח או חברה מנהלת, בקשר לענין, לרבות חוזה ביטוח או חוזה ביטוח או תקנון קות גמל, שבינהם לבין הלקוח לרבות מבוטח או עמית, בין אם התקשרו בעסקה ובין אם לאו".***

34. סעיף 4 לחוק תובענות ייצוגיות קובע את רשימת הזכאים להגיש בקשה לאישור תובענה ייצוגית. לענינו רלוונטי סעיף 4 (א)(1) לחוק:

"אדם שיש לו עילה בתביעה או בעניין כאמור בסעיף 3(א), המעוררת שאלות מהותיות של עובדה או משפט המשותפת לכלל החברים הנמנים עם קבוצת בני אדם- בשם אותה קבוצה."

35. כלומר, על מנת להיות זכאי להגיש בקשה לאישור תביעה ייצוגית, על מבקש להראות כי עומדת לו עילת תביעה באחד העניינים המנויים בתוספת השניה וכן כי התביעה מעוררת שאלות מהותיות של עובדה ומשפט המשותפות לכלל חברי קבוצת התובעים.

36. וליישום לענייננו, עלי להראות כי עומדת לזכותי עילת תביעה כנגד המשיבים, וכי עילת התביעה מעוררת שאלות משותפות של עובדה ומשפט לכלל חברי קבוצת התובעים.

37. בשלב של הבקשה לאישור תביעה ייצוגית על המבקש לשכנע את בית המשפט הנכבד כי עומדת לו לכאורה עילת תביעה אישית, אך אין להעמיד בהקשר זה דרישות מחמירות. עמדה על-כך השופטת שטרסברג כהן בע"א 2967/95 **מגן וקשת בע"מ נ' טמפו**, פ"ד נא(2) 312 (פסקה 19 לפסק-דינה):

> "נראה לי, כי על המבחן למילוי התנאים שבסעיף 54 מבחינת נטל ומידת ההוכחה, להיות אחיד לכל סעיפיו המשניים, ולגבי כל התנאים הנדרשים מהתובע, ועליו לשכנע את בית המשפט במידת הסבירות הראויה ולא על פי האמור בכתב התביעה בלבד, <u>כי הוא ממלא לכאורה</u> אחר כל דרישות סעיף 54א ולענייננו, שהראשונה בהן היא קיומה של עילה אישית כאמור בס' 54א(א). <u>אין להעמיד דרישות מחמירות מדי, לענין מידת השכנוע, משום שאלה עלולות להטיל על הצדדים ועל בית המשפט עומס יתר בבירור הנושא המקדמי, דבר העלול לגרום להתמשכות המשפט, לכפילות בהתדיינות ולרפיון ידים של תובעים ייצוגיים פוטנציאליים</u>. את כל אלה יש למנוע על ידי קריטריון מאוזן בנושא נטל ומידת ההוכחה הנדרשים מהתובע הייצוגי, שמצד אחד שלא יפטור אותו מחובת שכנוע ומצד שני לא יטיל עליו נטל כבד מדי.
>
> (ההדגשות אינן במקור – י.ג. וט.ר)

38. בנוגע להוכחת הנזק, חוק תובענות ייצוגיות קובע כי די בהוכחת גרימה של נזק ברמה לכאורית. כאמור בסעיף 4(ב)(1) לחוק:

"בבקשה לאישור שהוגשה בידי אדם כאמור בסעיף קטן 1(א) – די בכך שהמבקש יראה כי <u>לכאורה</u> נגרם לו נזק."

39. התנאים לאישור תביעה ייצוגית מנויים בסעיף 8(א) לחוק תובענות ייצוגיות, הקובע כי:

8. (א) בית המשפט רשאי לאשר תובענה ייצוגית, אם מצא שהתקיימו כל אלה:

(1) התובענה מעוררת שאלות מהותיות של עובדה או משפט המשותפות לכלל חברי הקבוצה, ויש אפשרות סבירה שהן יוכרעו בתובענה לטובת הקבוצה;

(2) תובענה ייצוגית היא הדרך היעילה וההוגנת להכרעה במחלוקת בנסיבות הענין;

(3) קיים יסוד סביר להניח כי ענינם של כלל חברי הקבוצה ייוצג וינוהל בדרך הולמת; הנתבע לא רשאי לערער או לבקש לערער על החלטה בענין זה;

(4) קיים יסוד סביר להניח כי ענינם של כלל חברי הקבוצה ייוצג וינוהל בתום לב.

40. בהתאם להוראות שפורטו לעיל, הרי שהדיון משלב זה יחולק לשני שלבים. **בשלב הראשון**, נראה כי עומדת לזכותי עילת תביעה אישית כנגד המשיבה, וכי נגרם לי נזק. **בשלב השני**, נעמוד על התקיימות התנאים לאישור התביעה כייצוגית המנויים בסעיף 8 לחוק תובענות.

(ב) <u>הפרת הוראות חוק הגנת הפרטיות ותקנות אבטחת המידע:</u>

41. נקבע **בע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' אריה ורדי** (23/01/2013 פורסם בנבו) בפסקה 22 לפסק דינו של כב' השופט פוגלמן:

"הזכות לפרטיות היא מהחשובות שבזכויות האדם בישראל. היא אחת החירויות המעצבות את אופיו של ההמשטר בישראל כמשטר דמוקרטי...ממועד קבלתו של חוק יסוד: כבוד האדם וחירותו, אף מוקנה לה מעמד חוקתי (ס' 7 לחוק היסוד) הפרטיות מאפשרת לאדם לפתח את עצמיותו ולקבוע את מידת המעורבות של החברה בהתנהגותו ובמעשיו הפרטיים. היא "מבצרו" הקנייני, האישי והנפשי"... הזכות לפרטיות, אם כן, מותחת את הקו בין הפרט אל הכלל, בין האני לבין החברה. היא משרטטת מתחם אשר בו מניחים את הפרט לנפשו לפיתוח האני שלו. בלא מעורבות של הזולת... היא "מגלמת את האינטרס היחיד שלא להיות מוטרד בצנעת חייו על ידי אחרים"

42. וכפי שפורט לכל אורך בקשה זו, קבעה הרשות להגנת הפרטיות – באופן רשמי, כי המשיבה הפרה את הוראות חוק הגנת הפרטיות, סעיף 17, ותקנות 2, 4, 5 (א), 9 (ב)(2), 10, 11 (S) ו- 14 (א), לתקנות אבטחת המידע בכך שלא שמרה כנדרש על המידע של מליון לקוחותיה, ופגעה בפרטיותם.

(ג) עוולת הרשלנות :

43. סעיפים 35-36 לפקודת הנזיקין קובעים באופן הבא :

רשלנות

"35. עשה אדם מעשה שאדם סביר ונבון לא היה עושה באותן נסיבות או לא עשה מעשה שאדם סביר ונבון היה עושה באותן נסיבות, או שבמשלח-יד פלוני לא השתמש במיומנות, או לא נקט מידת זהירות, שאדם סביר ונבון וכשיר לפעול באותו משלח-יד היה משתמש או נוקט באותן נסיבות - הרי זו התרשלות; ואם התרשל כאמור ביחס לאדם אחר, שלגביו יש לו באותן נסיבות חובה שלא לנהוג כפי שנהג, הרי זו רשלנות, והגורם ברשלנותו נזק לזולתו עושה עוולה.

חובה כלפי כל אדם

36. החובה האמורה בסעיף 35 מוטלת כלפי כל אדם וכלפי בעל כל נכס, כל אימת שאדם סביר צריך היה באותן נסיבות לראות מראש שהם עלולים במהלכם הרגיל של דברים להיפגע ממעשה או ממחדל המפורשים באותו סעיף."

44. עוולת הרשלנות מורכבת משלשה יסודות: קיום חובת זהירות, הפרת חובת הזהירות וגרימה של נזק . ראה ע"א 145/80 **ועקנין נ' המועצה המקומית בית שמש, פ"ד לז 1, 113, 112 (להלן:"עניין ועקנין")**.

45. לעניין קיומה של חובת זהירות איש לא יחלוק כי המשיבים חבים בחובת זהירות, הן מושגית והן קונקרטית, כלפי לקוחותיהם. המשיבים חבים בחובת זהירות, מושגית וקונקרטית, גם כלפי המבקשת.

46. בעניין ועקנין, נקבע כי קיומן של חובת זהירות מושגית וקונקרטית נקבעות בהתאם למבחן הצפיות במסגרתו יש לבחון האם אדם סביר מסוגל לצפות את הנזקים שנגרמו. לענייננו, איש לא יחלוק כי ניתן לצפות את האפשרות לגרימת נזקים בלתי ממוניים עקב פגיעה בפרטיותו לבטח הכלכלית, של מי שפרטי כרטיס האשראי שלו, שמו ומספר זהותו - נגנבים.

47. לעניין הפרת חבות הזהירות, הרי שאין כל ספק כי האירועים נשוא תובענה ייצוגית זו הינם פועל יוצא של התרשלותם של המשיבים . בהתאם לפסיקה, מוטלת החובה על מזיק לנקוט באמצעי זהירות סבירים. כפי שנקבע עניין ועקנין (עמ' 131) :

"חובתו של המזיק היא לנקוט אמצעי זהירות סבירים, ואחריותו מתגבשת, רק אם לא נקט אמצעים אלה. סבירותם של אמצעי הזהירות נקבעת על-פי אמות מידה אובייקטיביות, המגולמות באמירה, כי על המזיק לנהוג, כפי שאדם סביר היה נוהג בנסיבות העניין. אדם סביר זה אינו אלא בית המשפט, אשר צריך לקבוע את רמת הזהירות הראויה. רמת זהירות זו נקבעת על-פי שיקולים של מדיניות משפטית השאלה אינה, מהו האמצעי שמבחינה פיסית מונע נזק, אלא השאלה היא, מהו האמצעי שיש לדרוש כי ינקטו אותו בנסיבות העניין. על בית המשפט לאזן בין האינטרס של

הפרט הניזוק לביטחונו האישי, לבין האינטרס של המזיק לחופש פעולה, וכל זה על רקע האינטרס הציבורי בהמשכה או בהפסקתה של אותה פעולות. על בית המשפט להתחשב בסכנה ובגודלה. עליו להתחשב בחשיבותה החברתית של הפעולה. עליו לשקול את האמצעים הדרושים למניעתה"

48. לענייננו, על המשיבה היה לאבטח את פרטי לקוחותיה, וכל הפרטים שהיא לא שמרה עליהם.

49. אך מובן, כי במבחן התוצאה, הרי שהמשיבה לא אבטחה כראוי את הרשומות אשר במאגר המידע. משכך, פועל יוצא מכך, מובן כי המשיבה לא נקטו באמצעי זהירות זה, ובכך היא התרשלה.

50. ביחס לנזק, נגרם לי הן נזק כלכלי, והן נזק בלתי ממוני.

51. לעניין הנזק הממוני, היות והמשיבה מקבלת תמורה כספית מלקוחותיה, בגין השירות אותו היא נותנת, והשירות כולל בין היתר, כפי התחייבויותיה החוזיות, וכפי חובותיה הרגולטוריות, אף לשמור על פרטי לקוחותיה, וכל הפרטים האחרים, הרי שהיא הפרה את ההסכם כלפיה, ונתנה שירות חלקי, ולפיכך, עליה להשיב חלק יחסי מדמי הביטוח אותו היא גבתה מלקוחותיה, וחלק זה הנו 20% מדמי הביטוח שגבתה מכל לקוחותיה מ-7 השנים האחרונות.

52. אני סובר כי לאור האמור, יש לפצותי, בסכום של 500 ₪, המהווה 20% מהסכומים אותם שילמתי לידי המשיבה.

53. ביחס לנזק שאינו ממוני, הרי שאך מובן, שמרגע שהמשיבה, אחראית בשל התנהלותה, לאי אבטחת המידע של לקוחותיה, הם חברי הקבוצה, אשר בידיה ובמאגריה, הרי שבהתנהלותה, היא העמידה אותי ואת חברי הקבוצה, ועודה מעמידה אותנו – בסיכון כלכלי של ממש.

54. בשל העמדתי והעמדת חברי הקבוצה – בסיכון של ממש, וכן פגיעה ליבתית באוטונומיה של לקוחותיה, על המשיבה לפצות אותי ואת חברי הקבוצה, בסכום של 1,000 ₪.

55. סך נזקיי – הנם 1,500 ₪.

<u>**(ג) עילת הפרת חובת תום הלב**</u>

56. חובת תום הלב מהווה עיקרון חשוב החל על כל פעולה משפטית, וכן על ביצוע חיובים שאינם בגדר חוזה כהגדרתם בסעיף 61(ב) לחוק החוזים. מקום בו גוף כלכלי כדוגמת המשיבה הנותן שירות מכירתי לצרכנים ומכך נוצר לו רווח, הרי שמוטלת עליו נורמת התנהגות שהיא מעבר לחובת תום הלב הבסיסית.

57. **סעיף 12 לחוק החוזים מדבר על תום לב במשא ומתן:**

12. (א) במשא ומתן לקראת כריתתו של חוזה חייב אדם לנהוג בדרך מקובלת ובתום לב.
(ב) צד שלא נהג בדרך מקובלת ולא בתום-לב חייב לצד השני פיצויים בעד הנזק שנגרם לו עקב המשא ומתן או עקב כריתת החוזה, והוראות סעיפים 10, 13 ו-14 לחוק החוזים (תרופות בשל הפרת חוזה), תשל"א-1970, יחולו בשינויים המחוייבים.

58. **סעיף 39 לחוק החוזים מדבר על קיום בתום לב:**

39. בקיום של חיוב הנובע מחוזה יש לנהוג בדרך מקובלת ובתום לב; והוא הדין לגבי השימוש בזכות הנובעת מחוזה.

59. בת"א 2405/04 **בן עמי נ' הדר חברה לביטוח בע"מ** נקבע-

"הטעייה על-פי סעיף 2 לחוק יכול שתהא גם במחדל, כאשר גילויו של ענין מהותי לצרכן מתבקש בנסיבות הענין [...] החזקה היא כי הצרכן נותן אמון בעוסק; לא ניתן להטיל על הצרכן את הנטל לברר האם המוצר שרכש עונה על דרישות החוק או התקן".

(ההדגשות אינן במקור - י.ג וט.ר)

60. יצויין, כי ממהות ונסיבות עיסוקה של המשיבה והעובדה כי המשיבה עוסקת במתן שירות ו/או מכר לציבור גדול, יש להחיל עליה גם את עקרון "הדואליות הנורמטיבית" המחיל את עיקר כללי המשפט המנהלי, לרבות חובת תום לב מוגברת, חובת הגינות וכיוצ"ב (ר' ע"א 3414/93 **שמחה און נ' מפעלי בורסת היהלומים**, פורסם בנבו, 29.11.1995, פסקה 6):

"..לאחרונה עשתה הדואליות הנורמאטיבית צעד נוסף, גדול וחשוב. היא פרצה מן התחום של המינהל הציבורי אל התחום של המגזר הפרטי. בית המשפט פסק שהיא עשוייה לחול גם על גוף פרטי, שלא הוקם על-ידי חוק, אין לו סמכויות מכוח חוק ואין הוא משתייך, להלכה או למעשה, למינהל הציבורי...".

(ההדגשות אינן במקור - י.ג וט.ר)

61. מכל מקום, נראה כי המשיבה הפרה את סעיף 21.1 לתנאים הכללים של הסכם ההתקשרות שלה עם מבוטחיה, עת היא לא שמרה על כל הפרטים שלהם.

<u>(ו) עילת התעשרות שלא כדין:</u>

62. אין ולא יכול להיות כל ספק, כי עומדת לזכותי כנגד המשיבה עילת תביעה נוספת מכוח חוק עשיית עושר ולא במשפט, הואיל והמשיבה התעשרה על חשבוני ויתר חברי הקבוצה שלא כדין.

63. בהקשר זה, סעיף 1 **לחוק עשיית עושר ולא במשפט**, תשל"ט-1979 (להלן: **"חוק עשיית עושר"**) קובע כדלהלן:

"(א) מי שקיבל שלא על פי זכות שבדין נכס, שירות או טובת הנאה אחרת (להלן - הזוכה) שבאו לו מאדם אחר (להלן - המזכה), חייב להשיב למזכה את הזכייה, ואם השבה בעין בלתי אפשרית או בלתי סבירה - לשלם לו את שוויה."

64. הנה אם כן, חוק עשיית עושר קובע את העיקרון הבסיסי של חובת ההשבה, אשר נועד למנוע התעשרות שלא כדין של אדם על חשבון רעהו.

65. ודוק, חוק עשיית עושר איננו קובע רשימה סגורה של מצבים בהם נתונה הזכות להשבה, וכדבריו של כב' השופט, כתוארו אז, א' ברק בד"נ 20/82 **אדרס חומרי בנין בע"מ נ' הרלו אנד ג'ונס ג.מ.ב.ה**, פ"ד מב(1) 221, בעמ' 273:

"הקטגוריות של עשיית עושר ולא במשפט לעולם אינן סגורות ולעולם אינן שוקטות על השמרים... על השופט לפרש את הוראת המחוקק על פי תכלית החקיקה. התכלית היא, בין השאר, מניעת התעשרות שלא כדין... ביסוד תכלית זו עומדת התפיסה... לפיה יש להורות על השבה מקום שתחושת המצפון והיושר (ex aequo et bono) מחייבת השבה"

66. כך גם הבהירה כב' השופטת נתניהו בע"א 442/85 **משה זוהר ושות' נ' מעבדות טרבנול (ישראל) בע"מ**, פ"ד מד(3) 661, בעמ' 669:

"היתרון בכלי שנותן בידינו החוק הוא בגמישותו... אנו חופשיים להעניק את הסעד בכל מקרה ראוי שבו ההתעשרות מקוממת את חוש הצדק וההגינות והיא עונה בכך על היסוד 'שלא על פי זכות שבדין' שבסעיף 1(א) לחוק".

67. היסודות שיש להוכיח בעילה של עשיית עושר ולא במשפט, על פי סעיף 1 לחוק עשיית עושר הינם שלושה, כמפורט להלן:

(א) קבלה של נכס, שירות או טובת הנאה אחרת על ידי הזוכה (התעשרות).
(ב) ההתעשרות באה לזוכה מן המזכה או על חשבון המזכה (קשר סיבתי).
(ג) התעשרות הזוכה נעשתה "שלא על פי זכות שבדין" (יסוד נורמטיבי).
[לעניין זה ראה: ד"נ 20/82 הנ"ל, בעמ' 275, שם]

68. לענייננו, המשיבה עושה עושר כתוצאה מפעילותיה, בכך שהיא יוצרת אי וודאות ביחס לטיב מוצריה, ובכך יוצרת הטעייה והטיה של התנהלות צרכנית, ואין כל ספק שתוספת העושר כולה היא על גבם ועל חשבונם של חברי הקבוצה המיוצגת, עת היא נמנעה מלהשקיע כספים באבטחת המידע של לקוחותיה. ולפיכך, מחובתה להשיב לידי לקוחותיה את הסכום שאבטחת המידע הייתה עולה, לא הייתה מבצעת היא את כל הנדרש לשם שמירת פרטיותם של לקוחותיה.

69. האמור נכון אלפי מונים - אף ביחס למשיבה כחברת ביטוח.

70. כאמור המשיבה גורמת ללקוחותיה, לשלם עבור מוצר תקין וזאת ללא יידועם כי היא לא שומרת על פרטיות לקוחותיה, ופועלת לפי האינטרסים הכלכליים שלה.

ה. התקיימות התנאים לאישור התביעה כייצוגית

71. להלן נעמוד על התקיימות התנאים הקבועים בסעיף 8(א) לחוק התובענות הייצוגיות כסדרם.

פרטים הנוגעים לקבוצה

72. יובהר ראשית, תפקידו של בית המשפט הנכבד הוא להגדיר את קבוצת התובעים, כאמור בסעיף 10(א) לחוק התובענות הייצוגיות בו מצויין כי "אישר בית המשפט תובענה ייצוגית, יגדיר בהחלטתו את הקבוצה שבשמה תנוהל התובענה".

73. אני אטען כי מן הראוי שהקבוצה תכלול " כל אדם או אישיות משפטית אחרת, אשר הפרטים שלהם נכללו במאגר המידע של שירביט, ונחשפו, כתוצאה מהארועים הקשורים בדיווח של רשויות הביטוח והסייבר ו/או כל המבוטחים אשר הפרטים שלהם כלולים במאגר המידע של שירביט ואשר סבלו ו/או יסבלו מעוגמת נפש כתוצא מפרסום דבר פרשת דליפת המידע ו/או כל המבוטחים אשר הפרטים האישיים שלהם נכללו במאגר המידע של שירביט, והמידע השמור נפגם כולו או חלקו"".

74. מראש יצויין כי אין זה מחובתי להעריך במדויק את גודל הקבוצה ואת סכום הפיצוי המבוקש לכלל חברי הקבוצה, דבר שניתן יהיה לגלות במדויק רק לאחר חשיפת הנתונים ע"י המשיבה. ברי, כי אין בידי כל יכולת לדעת את כמות האנשים שנפגעים בענייננו זה.

75. חזקה על המשיבה, המוכרת ברבים כחברת ביטוח גדולה, כי כל נתון רלוונטי שמור במאגרי הנתונים שלה באופן שיטתי ומסודר, המאפשר את דלייתו בנקל.

76. במהלך הליך זה, אעתור, איפוא, לחיובה של המשיבה בחשיפת כל הנתונים הרלוונטיים ובכלל זאת מספר הלקוחות ונתוניהם האישיים.

זהו שמי זו חתימתי ותוכן תצהירי אמת.

חכם יהודה

חתימת המצהיר

<u>אישור עורך הדין</u>

אני החתום מטה, יוחי גבע, עו"ד מאשר כי ביום 1/12/2020 הופיע בפני מר יהודה חכם , ת.ז. 51884955, ולאחר שהזהרתיו כי עליו לומר את האמת כולה ואת האמת בלבד, וכי יהא צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר את נכונות התצהיר דלעיל וחתם עליו בפני.

יוחי גבע, עו"ד
מ.ר.
רחובות
08-9102344

חתימת עורך הדין

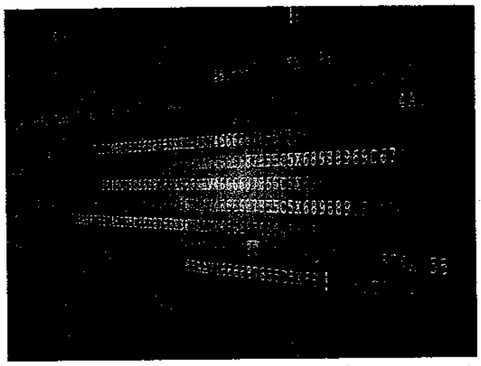
.3

הודעות לעיתונות

אירוע דלף מידע בחברת שירביט

תאריך פרסום: 01.12.2020

רשות שוק ההון, ביטוח וחיסכון ומערך הסייבר הלאומי מעדכנים על אירוע דלף מידע מחברת הביטוח שירביט



© Shutterstock

רשות שוק ההון, ביטוח וחיסכון ומערך הסייבר הלאומי מעדכנים על אירוע דלף מידע מחברת הביטוח שירביט. אמש החלו החברה בסיוע המערך לבדוק חשד לאירוע סייבר על אתר ושרתי החברה שבוצע על ידי האקרים.

מבדיקה ראשונית עולה כי מדובר במידע על פרטי ביטוח של לקוחות. במאמץ משותף לרשות ולמערך, הבדיקה ממשיכה. בעקבות כך שב וחידד המערך יחד עם הרשות את ההנחיות לגופים המוסדיים במשק.

אלו ההמלצות שלנו להגבהת חומות בארגונים:

1. וודאו קיום יכולת גיבוי והתאוששות מהירה של הארגון, בדגש על עותק עצמאי שאינו מחובר לרשת הארגון.

2. בצעו ניטור מוגבר, בדגש על אנומליות סייבר.

3. יש לצמצם עד למינימום הנדרש את משטח החשיפה לאינטרנט של הארגון - בדגש על ממשקי גישה מרחוק.

4. יש לוודא עדכון גרסאות למוצרים הנמצאים בממשק החוצה מהארגון.

5. בחינת הפעלת מערכות IDPS -Intrusion Detection and Prevention Services.

6. יש לבצע ניטור נפחי מידע היוצאים מהארגון במטרה לזהות ערוצי דלף אפשריים - בדגש על השוואה לתקופות קודמות דומות.

7. יש לחדד ערנות ולהעלות את המודעות של עובדי הארגון באשר לתכנים המתקבלים מגורמים בלתי מזוהים ועלולים להיות מתחזים.

עוד באותו נושא

ערכת הדרכה בנושא איומי סייבר ואבטחת מידע

דף זה עודכן לאחרונה בתאריך 01.12.2020

שירביט

טופס הצעה / אישור פרטים לביטוח רכב עובדי המדינה 2013

דף מס' 1

תקופת הביטוח מ- [illegible]/[illegible]/2013 עד 31/12/2013

א. פרטי עובד המדינה (חובה למלא חלק זה)

תעודת זהות

שם משפחה [illegible]

שם פרטי [illegible]

תאריך לידה

טלפון נייד

טלפון בבית

דואר אלקטרוני

רחוב

מספר הבית

עיר

תא דואר

טלפון בעבודה

פקס

מבוטח שהינו בן/בת זוג של עובד המדינה (יש למלא חלק זה רק במידה והינך מעוניין/ת שהפוליסה תופק על שמך והנך בן/בת זוג של עובד המדינה)

תעודת זהות

תאריך לידה

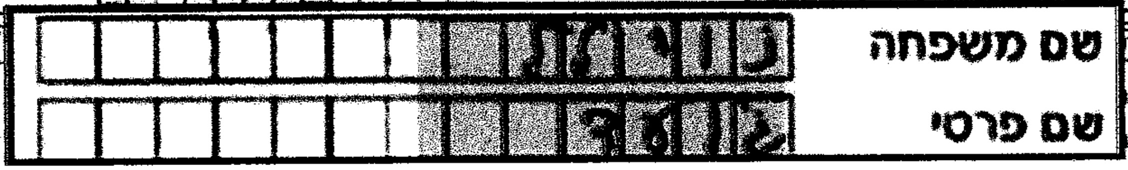
שם משפחה

שם פרטי

ב. פר...

סוג ה...

קוד ד...



שירביט

טופס הצעה / אישור פרטים לביטוח רכב עובדי המדינה 2013

דף מס' 1

תקופת הביטוח מ- 01/01/2013 עד 31/12/2013

א. פרטי עובד המדינה (חובה למלא חלק זה)

תעודת זהות [redacted] רחוב [redacted]
שם משפחה [redacted] מספר הבית דירה [redacted] כניסה
שם פרטי [redacted] עיר
תאריך לידה [redacted] תא דואר מיקוד [redacted]

סלולרי נייד [redacted] טלפון בעבודה 0
טלפון בבית [redacted] פקס 0
דואר אלקטרוני

מבוטח שהיה בן/בת זוג של עובד המדינה (יש למלא חלק זה רק במידה והינך מעוניין/ת שהפוליסה תונפק על שמך והנך בן/בת זוג של עובד המדינה)

תעודת זהות [redacted] שם משפחה [redacted]
תאריך לידה [redacted] שם פרטי [redacted]

ב. פרטי הרכב (נא לרשום את הפרטים מתוך פוליסה קודמת ו/או מרשיון הרכב)

סוג הרכב (נא סמן ב-X) [X] פרטי [ ] מסחרי תיבת הילוכים [ ] ידנית [X] אוטומטית
קוד דגם [redacted] שם היצרן/דגם [illegible] 1323
מספר רישוי [redacted] שנת יצור [illegible] מועד עליה לכביש [illegible]
נפח מנוע 13[illegible] מס' שילדה [redacted]

ג. סוג הכיסוי

סוג הכיסוי: [X] מקיף+חובה
משנת ייצור 1997 ומעלה

ד. פרטים נוספים (לצרכים סטטיסטיים בלבד)

אנא רשום את מספר התביעות, יש למלא את הספרה 0 (אפס) במידה ולא היו תביעות

מספר התביעות בשנה האחרונה: 0
מספר התביעות לפני שנתיים: 1
מספר התביעות לפני שלוש שנים: 1

מספר הנוהגים ברכב באופן קבוע: 2
המספר הכולל של שלילת הרשיון של כל נהגי הרכב ב-3 שנים אחרונות: 00
המספר הכולל של תאונות עם נפגעי גוף של כל נהגי הרכב ב-3 שנים אחרונות: 00

ה. פרטים לגבי המפעיל הצעיר ביותר הנוהג ברכב

תעודת זהות
שם משפחה
שם פרטי
תאריך לידה
תאריך הוצאת רשיון
מין [ ] זכר [ ] נקבה מצב משפחתי [ ] נשוי [ ] לא נשוי
האם המפעיל הצעיר ביותר הוא הנהג העיקרי של הרכב? [ ] כן [ ] לא
הרכב מצוייד במערכת A.B.S [ ] כן [ ] לא

ו. בחירת הכיסוי הביטוחי – למילוי בביטוי מקיף בלבד

בהתאם להוראות סכרת ביטוח רכב לעובדי מדינה לשנת 2012, באפשרותך לשאת בעלות פוליסה יותר של סבב דמי ההשתתפות העצמית בקרות אירוע ביטוחי, וזאת בכפוף למסלול הכיסוי שידרש על ידך, כמפורט להלן:

1. פוליסה ללא נהג צעיר (מעל גיל 24) – השתתפות עצמית בסך 500₪ בנוסף המדד, וסך של 900₪ במוסך שלא בהסדר עבור תשלום פרטיית בסיס בלבד.
(ביטוח חובה וביטוח מקיף) להלן – פרמיית הבסיס.
2. פוליסה לנהג מעל גיל 21 – השתתפות עצמית בסך 650₪ במוסך הסדר, וסך של 1,050₪ במוסך שאינו בהסדר (עבור תשלום בשיעור 110% מפרמיית הבסיס).
3. פוליסה לכל נהג – השתתפות עצמית בסך 900₪ במוסך הסדר, וסך של 1,200₪ במוסך שאינו בהסדר (עבור תשלום בשיעור 118% מפרמיית הבסיס).

לאור האמור, אנא סמן ב-X את גיל הנהג המבוקש על ידך:

1. [X] הנני בוחר בפוליסה ללא נהג צעיר (מעל גיל 24).
2. [ ] הנני בוחר בפוליסה לנהג מעל גיל 21.
3. [ ] הנני בוחר בפוליסה לכל נהג.

ההשתתפות העצמית תהא מוקרה ה נזק לרכב והוערך ע"י שמאי כי הוא מעל 6500₪.

לתשומת לבך: הכיסוי המוצע הינו כיסוי לכל נהג בביטוח רכב פרטי – נזקי רכוש ונזקי רכוש של צד ג' ("ביטוח מקיף"), בהתאם לכך, ויתור על הכיסוי לנהג הצעיר (מתחת לגיל 24 או מתחת לגיל 21) משמעותו כי פוליסת ביטוח המקיף לא תכסה מקרה ביטוח שנגרם בעקבות נהיגתו של מי שגילו מתחת ל-24 או 21, לפי העניין. יחד עם זאת, באפשרותך לבקש מחברת הביטוח להוסיף, בכל עת, כיסוי ביטוחי עבור נהג שגילו מתחת לגיל 24 או 21, לפי בחירתך וככל שתראה בכך צורך.

תאריך: ______ חתימת המבוטח: X ______

61740

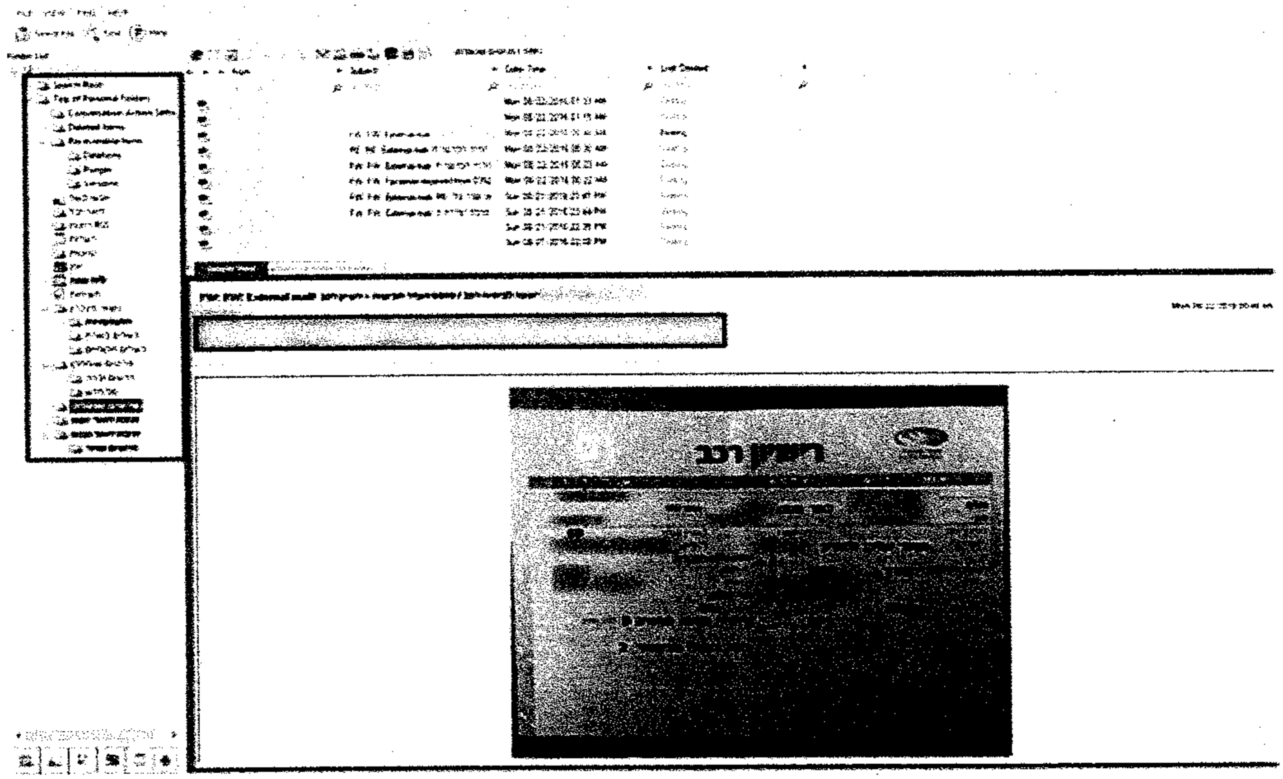
Network ▸ 172.58.0.30 ▸ d$ ▸ Backup ▸ Exchange Servers

Organize ▾ Open New folder

Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network

Date modified	Name	Type	Size
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	VIB File	[illegible]
11/24/2020 ...	Exchange Servers ShabakMBX01D2020-11-24T1419...	VIB File	154,164,13...
11/4/2020 7:...	Exchange Servers ShabakMBX01D2020-11-04T1755...	VIB File	119,558,03...
11/12/2020 ...	Exchange Servers ShabakMBX01D2020-11-12T1617...	VIB File	90,016,653...
11/10/2020 ...	Exchange Servers ShabakMBX01D2020-11-10T1440...	VIB File	88,944,178...
11/6/2020 5:...	Exchange Servers ShabakMBX01D2020-11-06T1641...	VIB File	86,512,543...
11/1/2020 1:...	Exchange Servers ShabakMBX01D2020-11-01T2141...	VIB File	81,639,472...
10/27/2020 ...	Exchange Servers ShabakMBX01D2020-10-27T2119...	VIB File	80,110,859...
11/5/2020 4:...	Exchange Servers ShabakMBX01D2020-11-05T1557...	VIB File	79,917,495...
11/17/2020 ...	Exchange Servers ShabakMBX01D2020-11-17T1517...	VIB File	79,351,708...
11/11/2020 ...	Exchange Servers ShabakMBX01D2020-11-11T1419...	VIB File	76,847,726...
11/15/2020 ...	Exchange Servers ShabakMBX01D2020-11-15T1608...	VIB File	75,835,972...
11/18/2020 ...	Exchange Servers ShabakMBX01D2020-11-18T1443...	VIB File	72,838,374...
10/25/2020 ...	Exchange Servers ShabakMBX01D2020-10-25T2300...	VIB File	72,579,609...
11/19/2020 ...	Exchange Servers ShabakMBX01D2020-11-19T1546...	VIB File	72,479,436...
10/29/2020 ...	Exchange Servers ShabakMBX01D2020-10-29T1852...	VIB File	71,951,907...
11/16/2020 ...	Exchange Servers ShabakMBX01D2020-11-16T1500...	VIB File	70,313,139...
10/27/2020 ...	Exchange Servers ShabakMBX01D2020-10-26T2314...	VIB File	68,686,627...
11/21/2020 ...	Exchange Servers ShabakMBX01D2020-11-21T1053...	VIB File	67,763,318...
11/2/2020 5:...	Exchange Servers ShabakMBX01D2020-11-02T1609...	VIB File	67,309,475...
11/14/2020 ...	Exchange Servers ShabakMBX01D2020-11-14T1052...	VIB File	64,947,314...
11/25/2020 ...	Exchange Servers ShabakMBX01D2020-11-25T1820...	VIB File	64,457,379...
10/28/2020 ...	Exchange Servers ShabakMBX01D2020-10-28T1930...	VIB File	63,621,360...
11/7/2020 8:...	Exchange Servers ShabakMBX01D2020-11-07T0759...	VIB File	63,441,692...
11/9/2020 3:...	Exchange Servers ShabakMBX01D2020-11-09T1444...	VIB File	61,282,816...
10/31/2020 ...	Exchange Servers ShabakMBX01D2020-10-31T1246...	VIB File	50,676,601...
10/24/2020 ...	Exchange Servers ShabakMBX01D2020-10-24T0905...	VIB File	41,648,916...
11/29/2020 ...	Exchange Servers ShabakMBX01D2020-11-29T1329...	VIB File	40,663,104...
10/25/2020 ...	Exchange Servers ShabakMBX01D2020-10-25T0250...	VIB File	30,094,992...
11/14/2020 ...	Exchange Servers ShabakMBX01D2020-11-14T2224...	VIB File	23,438,644...
11/28/2020 ...	Exchange Servers ShabakMBX01D2020-11-28T0428...	VIB File	17,329,131...
11/1/2020 1:...	Exchange Servers ShabakMBX01D2020-11-01T0000...	VIB File	14,884,512...
11/29/2020 ...	Exchange Servers ShabakMBX01D2020-11-29T0301...	VIB File	12,747,317...
11/7/2020 5:...	Exchange Servers ShabakMBX01D2020-11-07T1745...	VIB File	11,294,989...
11/21/2020 ...	Exchange Servers ShabakMBX01D2020-11-21T2200...	VIB File	6,924,045 KB
11/29/2020 ...	Exchange Servers.vbm	VBM File	1,305 KB

Exchange Servers ShabakMBX01D2020-11-2... Date modified: 11/27/2020 2:27 PM Date created: 11/27/2020 2:31 AM
VBK File Size: 929 GB



@blackshadow

מדינת ישראל
משרד התחבורה, התשתיות הלאומיות והבטיחות בדרכים
רשות הרישוי

רשיון לרכב

מס' [redacted] 181 פרטי מסמך [redacted]

שם [redacted]

[redacted]

מועד עליה לכביש [redacted]

[illegible] [redacted]

[illegible]	[illegible]	ABS	[illegible]	חלון גג	[illegible]	הוראות רישום	[illegible]
[redacted]						[redacted]	[redacted]

[redacted]

2013

[redacted]

רשיון לרכב [illegible]

נכון ל- 29/11/2020

ענף : 227 - חשכ"ל-פרטי/מסחרי עד 3.5ט'

סוכן
מספר רישוי
ת.ז./ח.פ.

מבוטח/ת נכבד/ה

הנדון: דיווח על תביעות במהלך 3 השנים האחרונות

במתחייב מתקנות הפיקוח על עסקי ביטוח הננו לפרט להלן את התביעות שהוגשו לחברתנו, עד לתאריך הדפסת מכתב זה, על-ידך או בגין הביטוח שניתן בפוליסה להלן, במשך תקופת הביטוח המפורטת:

פוליסה: [illegible]-מקיף   תקופת ביטוח: מ-1/01/2018 עד-31/12/2018

מס. רישוי	מס. תביעה	מועד מקרה ביטוח	סוג תביעה	סכום ששולם(בש"ח)	מצב
1	[illegible]	26/02/2018	נזק ישיר - [illegible]	27,920.00	סגורה
סוג מובטח:צד שלישי		שיבוב: לא	סכום ירידת ערך:		

בכבוד רב
שירביט חברה לביטוח בע"מ

@blackshadowsleaks

מדינת ישראל
משרד האוצר - אגף שוק ההון, ביטוח וחסכון

כ״ז באב התשע״ו
31 באוגוסט 2016

5

חוזר גופים מוסדיים 2016-9-14
סיווג: כללי

ניהול סיכוני סייבר בגופים מוסדיים

בתוקף סמכותי לפי סעיפים 2(ב) ו-42 לחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ״א-1981, סעיף 39(ב)(1) ו-40 לחוק הפיקוח על שירותים פיננסיים (קופות גמל), התשס״ה-2005 ותקנה 8(א)(20) לתקנות הפיקוח על שירותים פיננסיים (דירקטוריון וועדותיו), התשס״ז-2007 ולאחר התייעצות עם הוועדה המייעצת, להלן הוראותיי:

1. כללי

עם ההתפתחות הטכנולוגית ותלותן של פעילויות עסקיות ברשת האינטרנט גדלו היקפם ועוצמתם של איומים קיברנטיים העלולים לשבש את פעילותם התקינה של גופים מוסדיים. על כן, עלה הצורך לעדכן את תפיסת ההגנה של גופים מוסדיים כך שתינתן התייחסות גם לאיומים אלו.

אם בעבר תפיסת ההגנה התייחסה לאבטחת מידע, דהיינו הגנה על המידע בהיבט של סודיות, שלמות וזמינות המידע, הרי שכיום אבטחת מידע הנה רק רובד אחד בתוך תחום ניהול סיכוני הסייבר עליו יש להגן. לצד הגנה על המידע, עולה הצורך להגן גם מפני שיבוש פעילותו התקינה של הרכיב הממוחשב עליו מתבסס הגוף המוסדי.

מטרת חוזר זה הינה לקבוע עקרונות להגנה על נכסי הגוף המוסדי במטרה להבטיח את שמירת זכויות העמיתים והמבוטחים על ידי שמירה על סודיות, שלמות וזמינות נכסי המידע, מערכות המידע, התהליכים העסקיים ופעילותו התקינה של הגוף המוסדי. ניהול סיכוני הסייבר יכלול פעולות של מניעה, נטרול, חקירה והתמודדות עם איומי ואירועי סייבר במטרה לצמצם את השפעתם והנזק הנגרם מהם, בטרם התרחשותם, במהלכם ולאחריהם.

החוזר מגדיר עקרונות לניהול סיכוני סייבר בגוף מוסדי ומחייב לנהל סיכונים אלו. על הגופים המוסדיים לנהל את סיכוני הסייבר באופן אפקטיבי, עדכני ושוטף, ועל בסיס עקרונות ממשל תאגידי נאותים הכוללים התייחסות לשיטות, לתהליכים ולבקרות ובאופן אשר יאפשר להם להתמודד עם איומי סייבר ולנהל אירועי סייבר.

לאור מרכזיות גופים מוסדיים בשוק ההון הישראלי, ולאור הסיכון הגבוה בתחום הגנת הסייבר, מצופה מגוף מוסדי לאמץ סטנדרטים גבוהים בתחום זה.

רח׳ קפלן 1, ירושלים 9103002 ת.ד. 3100 טל׳ 02-5317111 פקס׳ 02-5695342
www.mof.gov.il

תוכן עניינים

1. כללי 1
2. הגדרות 4
3. ממשל תאגידי 6
   א. תפקידים ותחומי אחריות 6
      1) דירקטוריון גוף מוסדי 6
      2) מנכ"ל גוף מוסדי 6
      3) ועדת היגוי לניהול סיכוני סייבר 6
      4) מנהל הגנת סייבר 7
   ב. מסגרת ניהול סיכוני סייבר (Framework) 7
      1) מדיניות 7
      2) נהלים 8
      3) תכנית עבודה 8
4. ניהול הסיכון 8
   א. הערכת סיכונים ועדכניותה 8
   ב. דיווח וניטור סיכונים 9
   ג. יישום בקרות 9
5. הגנת סייבר של גוף מוסדי 9
   א. הגנת סייבר, ניטור ובקרה 9
      1) איסוף מודיעין 9
      2) ניטור ובקרת מערכות מידע 10
      3) מוכנות לאירועים 10
   ב. ביצוע סקרים 11
      1) סקרים ומבחני חדירה 11
      2) טיפול בממצאי סקרים ומבחני חדירה 12
   ג. אבטחת מערכות, תקשורת ותפעול 12
      1) אבטחת רשת וגישה מרחוק 13
      2) קישוריות גוף מוסדי לרשת האינטרנט 13
      3) הוצאת נתונים אל מחוץ לחצרותיו 13
      4) הצפנה 13
      5) אבטחת מערכות ועדכונן 13
      6) אבטחת מערכות קצה 14
      7) מניעת קוד עוין 14
      8) הגנת סייבר בתהליכי רכש ופיתוח 14
      9) הפרדה בין סביבות ואבטחתן 15
   ד. ניהול משתמשים והרשאות 15

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

1) ניהול משתמשים 15
2) סיסמאות ואמצעי הזדהות 15
3) ניהול הרשאות ובקרת גישה 16
ה. מיקור חוץ (Outsourcing) 16
1) דרישות הגנת סייבר בהסכמי מיקור חוץ 16
2) שירות למערכות גוף מוסדי על ידי נותן שירות מיקור חוץ 16
3) שירותי מחשוב ענן 17
ו. אבטחה פיסית וסביבתית 17
1) אזורים מאובטחים 17
2) אבטחת ציוד וניירת 18
ז. הגנת סייבר במשאבי אנוש וגיוס עובדים 18
1) הגנת סייבר בתהליך גיוס עובדים 18
2) אבטחת מידע בעת מעבר תפקיד או סיום העסקת עובדים 18
3) מודעות הגנת סייבר והדרכה 18
6. אבטחת ערוצי קשר עם לקוחות 19
א. אבטחת ערוצי תקשורת מבוססי אינטרנט 19
ב. רישום מבוטחים/עמיתים לפעילות 19
1) וידוא זהות בתהליך הרישום 19
2) הסכמה מפורשת של לקוחות בטרם רישום לפעילות 19
ג. הזדהות לקוחות לערוצי שירות 20
ד. שליחת מידע באמצעים דיגיטליים 20
ה. שיווק מוצרים באמצעים דיגיטליים (ומסחר דיגיטלי) 20
7. אבטחת ערוצי קשר עם גורמים חיצוניים 20
א. אבטחת ערוצי קשר בין גופים מוסדיים לבין בעלי רישיון 20
ב. אבטחת ערוצי קשר בין גופים מוסדיים 21
8. החלת ההוראה 21
א. תחולה 21
ב. תחילה 21
ג. ביטול תקפות 21

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

2. הגדרות

"איום – Threat" – אפשרות פוטנציאלית לפגיעה בסודיות, שלמות, או זמינות המידע.

"אירוע סייבר" – כל מקרה של תקיפת מערכות או אמצעי טכנולוגי אחר ששייכים לגוף מוסדי, העלולה לפגוע בסודיות, שלמות או זמינות מערכות או המידע של גוף מוסדי.

"אמצעי זיהוי" – אמצעי המאפשר אימות פרטים של אדם או מערכת בעת ניסיון גישה או ביצוע פעולות מטעמם במערכת מידע.

"בעל רישיון" – כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ייעוץ, שיווק, ומערכת סליקה פנסיונית), התשס"ה-2005 ולרבות "סוכן ביטוח" או "סוכן" כהגדרתם בחוק הפיקוח על שירותים פיננסיים (ביטוח) תשמ"א-1981.

"גוף מוסדי בעל היקף פעילות נמוך" – כהגדרתו בשער 1 לחוזר המאוחד - הגדרות.

"גישה מרחוק – Remote Access" – התחברות גורם (חיצוני או פנימי) מחוץ לרשת הארגון אל הרשת הפנימית של הארגון.

"הזדהות חזקה – Strong Authentication" – מבוססת על שימוש באמצעי זיהוי המתבסס על לפחות שניים מתוך הפריטים הבאים:

א. Something You Are – תכונה פיזיולוגית ייחודית של המשתמש.

ב. Something You Have – פריט הנמצא ברשות המשתמש.

ג. Something You Know – פריט מידע הידוע למשתמש.

"הערכת סיכונים" – תהליך של הערכת רמת הסיכון של כלל המידע, מערכות המידע והתהליכים העסקיים והטכנולוגיים בגוף. התהליך ממפה את הסיכונים השונים הנובעים מהפעילות והתהליכים בגוף המוסדי.

"הצפנה" – המרת מידע גלוי (Clear Text) למידע מוצפן (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

"טוקניזציה" – תהליך המרת נתונים רגישים בערכים חלופיים שאינם רגישים ("טוקנים") אשר אין סכנה בחשיפתם. לרוב, תהליך זה מבוצע על ידי מערכת המחליפה את הערך המקורי בערך חלופי, ומאפשרת את שחזור הערך המקורי בעת הצורך, ובאופן מוגבל.

"זיהוי חד ערכי" – ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

"יעד התאוששות (RTO - Recovery Time Objective)" – יעד אותו קבע גוף מוסדי להחזרת פעילות עסקית ספציפית ומערכות התומכות בה לרמת שירות מוגדרת בפרק זמן מוגדר;

"יעד שירות" – רמת שירות לעמיתים או למבוטחים במצב חירום שעליה החליט דירקטוריון גוף מוסדי;

"לוג - Log" – קובץ התיעוד של נתיב בקרה, מכיל פרטים בנוגע לפעולות הממוחשבות המבוצעות בארגון.

"מידע רגיש" – כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981, וכל מידע אשר סווג על ידי הגוף כרגיש.

"מיסוך נתונים" – טכנולוגיה המבצעת הסתרה של נתונים או חלק מהם אשר הוגדרו סודיים, כך שבעת הצגת נתון, הוא מוחלף ברצף תווים אחר. שימוש בטכנולוגית מיסוך מאפשר לעבד נתונים כך שהצפייה בהם תהיה מוגבלת לגורמים מועטים בלבד.

"מערכות ליבה" – המערכות שהוגדרו על ידי גוף מוסדי כמערכות מרכזיות של הארגון ואושרו ככאלה על ידי הדירקטוריון, לרבות כל מערכת אשר יש לה השפעה ישירה על זכויות עמיתים ומבוטחים וכל מערכת שהמידע המנוהל בה עשוי להשפיע באופן מהותי על עסקי הגוף המוסדי ויציבותו, בין היתר, לרבות המערכות שלהלן וכל אחת מאלה:

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

א. מערכות ביטוח חיים;

ב. מערכות ביטוח כללי;

ג. מערכות ביטוח בריאות;

ד. מערכות תפעול זכויות עמיתים ומבוטחים;

ה. מערכות ההשקעות והפיננסים;

ו. מערכות מקבילות ו/או מערכות התומכות מהותית בפעילות המערכות המפורטות לעיל כגון: מערכת הכספים, מערכת אקטוארית, מערכת תביעות, מערכת ביטוח משנה וכדי.

"מערכות מידע" – כלל המערכות התומכות בפעילות העסקית בגוף מוסדי, לרבות ציוד ממוכן, תשתיות וטכנולוגיות התומכות בתפעולן, בין השאר: שרתים, ציוד תקשורת, ציוד הגנת סייבר.

"מערכות OT (Operation Technology)" – מערכות (לרבות תוכנה וחומרה) המיועדות לשליטה ובקרה של מערכות תעשייתיות או אוטומציה (באמצעות בקרה ושליטה ישירה) של התקנים פיזיים.

"נכסי מידע" – נכס מידע הוא מאגר נתונים, התקן, או רכיב של סביבה התומך בפעילויות הקשורות במידע (לרבות תשתיות). נכסי מידע כוללים, בדרך כלל, חומרה, תוכנה ומידע.

"נתיב בקרה" – תיעוד פעולות המתבצעות במערכות מידע. התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד, לצורך זיהוי האלמנטים שהשתנו.

"סייבר", "המרחב הקיברנטי" – המתחם הפיזי והלא פיזי שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות וממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה ולרבות רובד אנושי (האנשים המשתמשים בכל אלה). הגנת סייבר כוללת בתוכה את כלל היבטי אבטחת המידע.

"סיכון סייבר" – סיכון לשימוש לא מורשה בזהות, הפרעה לפעילות על ידי פגיעה בפעילות הרשת או השבתת שירותים, פגיעה במערכות, גניבה של נכסים דיגיטליים, החדרה של קודים או תוכנות זדוניות, חדירה למערכת או חשיפת מידע.

"סיכון שורשי" – סיכון מובנה. מאפיין את פעילות הגוף ללא תלות באמצעי הגנת סייבר המיושמים בגוף.

"סיכון שיורי" – סיכון שנותר לאחר יישום בקרות ואמצעי הגנת סייבר בגוף.

"סקר סיכונים" – תהליך שמטרתו זיהוי האיומים, הערכת הסיכון הנובע מהם (תוך התחשבות בסבירות התממשותם והנזק הפוטנציאלי כתוצאה מכך) וזיהוי הבקרות הנדרשות לצמצום סיכונים אלה.

"סריקת חשיפות אבטחת מידע – Vulnerability Scan" – סריקה לאיתור חולשה במערכת העלולה להוביל להתממשות איום.

"קוד עוין" – קוד המושתל על ידי משתמש זדוני ועשוי לגרום לביצוע פעולות לא רצויות, פגיעה במערכות הארגון וזליגת מידע רגיש לגורמים לא מורשים.

"הצפנה מקצה לקצה" – הצפנת תווך התקשורת או הנתונים מהתחנה או השרת (למשל: תחנת עבודה של משתמש) היוזמת את השירות אל התחנה או השרת (למשל: מערכת מידע) המספקת את השירות.

"רשת פנימית – Local Area Network (LAN)" – קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים בתוך הארגון. במובן של הוראה זו, רשת פנימית הנה רשת המופרדת מרשתות ציבוריות.

"תווך תקשורת ציבורי – Public Network" – תשתיות תקשורת המשרתות או משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם. תשתיות אינטרנט מוגדרות כתווך תקשורת ציבורי.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

"תעודת הצפנה – SSL Certificate" – תעודה הניתנת על ידי "רשות אמון" המאשרת את אמינות החיבור ומאמתת את מהימנות מקור החיבור.

"DNS" – שרות הממיר כתובות IP לכתובות מילוליות(URL) ובכך מקל את השימוש ברשת האינטרנט.

3. ממשל תאגידי

א. תפקידים ותחומי אחריות

1) דירקטוריון גוף מוסדי

א) יאשר מדיניות כאמור בסעיף 1.ב.3) בתחום ניהול סיכוני סייבר, לכל הפחות אחת לשנה.

ב) ידון בתכנית מעודכנת לניהול סיכוני סייבר והערכת סיכונים, הכוללת תכנית להפחתת סיכונים ופירוט השינויים במסגרת ניהול תחום סיכוני הסייבר, לכל הפחות אחת לשנה.

ג) יאשר את כתב מינוי ועדת ההיגוי בתחום סיכוני סייבר שבמסגרתו יוגדרו תפקידיה וסמכויותיה של הוועדה כאמור בסעיף 3.א.3) להלן.

2) מנכ"ל גוף מוסדי

א) יבטיח את ניהולו התקין של תחום סיכוני הסייבר בהתאם ליעדים, למדיניות ולצורכי הגוף המוסדי.

ב) יקיים מסגרת נהלים בהתאם לאמור בסעיף 2.ב.3) ויאשר תכנית עבודה שנתית בתחום ניהול סיכוני סייבר בהתאם לאמור בסעיף 3.ב.3).

ג) יעמיד משאבים נאותים ליישום תכנית עבודה לניהול סיכוני סייבר.

ד) יקיים מבנה ארגוני הולם לניהול סיכוני סייבר ויגדיר את אחריות הגורמים העוסקים בתחום ואת הממשקים ביניהם, תוך שמירה על עקרונות של הפרדת תפקידים וסמכויות.

ה) יקיים מנגנוני בקרה ופיקוח נאותים בתחום ניהול סיכוני סייבר.

ו) יקבע הוראות דיווח אליו ולגורמים רלוונטיים אחרים בעת אירועי סייבר.

ז) ידון בהמלצות ועדת ההיגוי בהתאם לאמור בסעיף 3.א.3(ח).

ח) יבחן אימוץ תקן ת"י ISO 27001 של מכון התקנים הישראלי.

3) ועדת היגוי לניהול סיכוני סייבר

א) גוף מוסדי ימנה ועדת היגוי ובראשה יעמוד המנהל הכללי של הגוף המוסדי ובין חבריה יכללו מנהל מערכות המידע, מנהל הסיכונים ומנהל הגנת הסייבר.

ב) יכול שהמנהל הכללי של הגוף המוסדי לא יעמוד בראש ועדת ההיגוי, ובלבד שהתקיים דיון בהנהלת הגוף המוסדי בו הוצגו הנימוקים לבחירתו של חבר הנהלה אחר בעל כישורים מתאימים.

ג) בגוף מוסדי בעל היקף פעילות נמוך יכול שלא תוקם ועדת היגוי לניהול סיכוני סייבר ובלבד שכל תפקידי הוועדה שיפורטו להלן יועברו לאחריות המנכ"ל.

ד) קבוצת חברות שהינן תחת אותו בעל שליטה, יכולה לקיים ועדת היגוי אחת לקבוצת החברות (להלן – ועדת היגוי קבוצתית) ובלבד שהגורמים המוסמכים לכך בכל גוף מוסדי בקבוצה, יאשרו את מינוי ועדת ההיגוי הקבוצתית כוועדת ההיגוי של הגוף המוסדי. בהינתן ומונתה ועדת היגוי קבוצתית, ניתן שיתקיימו דיונים משותפים הרלוונטיים לכל חברות הקבוצה ובלבד שבנוסף, יתקיימו דיונים בנושאים פרטניים הייחודיים לכל חברה בקבוצה, בנושאים שבהם נדרש גוף מוסדי בקבוצה לדון בוועדת ההיגוי, בהתאם להוראות חוזר זה. לדיונים הפרטניים

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

יוזמנו כל הגורמים שהוגדרו בחוזר זה וגורמים שהוסמכו לכך מטעם הגוף המוסדי שבקבוצת התברות.

ה) הוועדה תתכנס לכל הפחות אחת לרבעון ותערוך פרוטוקולים של ישיבותיה.

ו) הוועדה תסייע למנהל הכללי לקבל החלטות ולבצע את תפקידיו בכל הקשור לניהול התקין של תחום ניהול סיכוני סייבר, מתוך ראיה אינטגרטיבית של התחום ברמה כלל ארגונית.

ז) הוועדה תבצע מעקב אחר יישום תכנית העבודה בתחום ניהול סיכוני סייבר.

ח) הוועדה תדון בתוצאות הערכת סיכונים ובתכנית להפחתתם בהתאם לאמור בסעיף 4.ב..

ט) הוועדה תדון בסיכונים אפשריים בהפעלת שימוש במערכות מבוססות ענן בהתאם לאמור בסעיף 5.ה.3)א).

י) הוועדה תתחקר ותפיק לקחים לגבי כל אירוע סייבר משמעותי בהתאם לאמור בסעיף 5.א.2)י).

יא) הוועדה תדווח לדירקטוריון הגוף המוסדי, לכל הפחות אחת לשנה, על פעילותה, מסקנותיה והמלצותיה בנושאים שהוסמכה לעסוק בהם.

יב) ועדת היגוי שבראשה עומד חבר הנהלה אחר מהמנהל הכללי, תדווח למנהל הכללי על סטטוס ביצוע תכנית העבודה אחת לרבעון ותעביר לו את המלצותיה בעניין תוצאות הערכת סיכונים והתכנית להפחתתם בהתאם לאמור בסעיף 4.ב. ולגבי כל אירוע סייבר משמעותי בהתאם לאמור בסעיף 5.א.2)י).

4) מנהל הגנת סייבר

א) גוף מוסדי ימנה מנהל הגנת סייבר בעל מומחיות וניסיון מוכחים בתפקיד ניהולי בתחום הגנת הסייבר.

ב) מנהל הגנת סייבר לא ימלא כל תפקיד שעלול לפגוע ביכולתו לבצע כראוי את תפקידו כמנהל הגנת סייבר או להגבילה, ויהיה כפוף לאחד מחברי ההנהלה החברים בוועדת ההיגוי.

ג) חבר ההנהלה הממונה על מנהל הגנת סייבר יהיה אחראי על הפעילות המתבצעת בתחומי ניהול סיכוני הסייבר וכן על בקרת תכנית העבודה בנושא זה, בהתאם למדיניות ניהול סיכוני הסייבר של הגוף המוסדי.

ד) מנהל הגנת סייבר יפעל ליישום מדיניות בתחום ניהול סיכוני סייבר בגוף המוסדי, ייעץ וינחה את הגוף מוסדי בנושאי הגנת סייבר, יקבע נהלי עבודה, ומסגרת דיווחים ויבצע פיקוח ובקרה בנושאים אלו והכל בהתאם להוראות חוזר זה.

ה) למנהל הגנת סייבר יוקצו המשאבים והמקורות הנאותים לביצוע תפקידו.

ב. מסגרת ניהול סיכוני סייבר (FRAMEWORK)

1) מדיניות

גוף מוסדי יגדיר מדיניות לניהול סיכוני סייבר הקובעת עקרונות מנחים להגנת סייבר ליישום בגוף. עקרונות אלו יתייחסו, בין היתר, ליעדים שהוגדרו, למסגרת ארגונית (תחומי אחריות, קווי דיווח, פיקוח ובקרה), ליישום הגנת סייבר בהיבט של מחשוב ענן (סוגי השירותים והיקפם, אחריות, פיקוח ובקרה), ליישום הגנת סייבר בהיבטי משאבי אנוש (מהימנות עובדים, הדרכה ובקרה), ליישום הגנת סייבר פיסית ולוגית בתהליכים, במערכות ובתשתיות הגוף ולכל הנושאים שיש להם השפעה רוחבית על יחידות גוף מוסדי.

2) נהלים

א) גוף מוסדי יקבע נהלים המגדירים את תהליכי הגנת הסייבר בגוף והמתייחסים לנושאים המפורטים בהוראה זו ויפעל להטמעתם.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) הנהלים ייגזרו ממדיניות ניהול סיכוני סייבר ומהנחיות חיצוניות (כגון אסדרה או מחויבויות חוזיות).

ג) גוף מוסדי יגדיר נוהל לדרישות הגנת סייבר ביחס לסיכוני מיקור חוץ בהתאם לאמור בסעיף 5.ה.1(א).

ד) הנהלים יעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או שינוי במתאר הסיכונים של הגוף המוסדי, ולכל הפחות אחת ל – 24 חודשים.

3) **תכנית עבודה**

תכנית העבודה תיגזר ממדיניות ונהלי סיכוני סייבר של גוף מוסדי. התכנית תתייחס לאופי המידע, לתהליכים, לתשתיות ולמערכות הגוף המוסדי ותכלול, לכל הפחות, תכנית לניהול סיכוני סייבר כאמור בסעיף 4, לרבות תכנית להפחתתם, תכנית להעלאת רמת מודעות העובדים בהתאם לאמור בסעיף 5.ז.3), תכנית לביצוע סקרים בהתאם לאמור בסעיף 5.ב.1)ד) ותכנית היערכות וניהול אירועי סייבר בהתאם לאמור בסעיפים 5.א.3(ב) – 5.א.3(ד).

4. ניהול הסיכון

גוף מוסדי יגדיר תכנית לניהול סיכוני סייבר, שתעסוק בסיכונים לתהליכים, למערכות ולמידע ותתבצע בהתאם לסעיפים שלהלן:

א. הערכת סיכונים ועדכניותה

1) גוף מוסדי יעריך את סיכוני הסייבר כדי לספק תמונת מצב עדכנית של מכלול הסיכונים שהוא מתמודד עמם.

2) הערכת הסיכונים תכלול, בין היתר, את השלבים הבאים:
   א) זיהוי תהליכים, מערכות ונכסי מידע.
   ב) מיפוי סיכונים לתהליכים, מערכות ולנכסי מידע כאמור.
   ג) מיפוי סיכונים שורשיים.
   ד) מיפוי והערכת הבקרות למזעור סיכונים אלה, לרבות בחינה של מידת השפעת הבקרות עליהם.
   ה) הערכת סיכון שיורי (בהתאם להשפעת הבקרות שיושמו).

3) לצורך זיהוי והערכת הסיכונים, גוף מוסדי ישתמש, בין היתר, בממצאי ביקורות וסקרים, איסוף וניתוח אירועי סייבר שהתרחשו בגוף המוסדי בעבר וניתוח תרחישים לזיהוי אירועים פוטנציאליים של התממשות הסיכון.

4) הערכת הסיכונים תתייחס בין היתר למערכות OT ולסביבות פיתוח ובדיקות, העשויות להכיל מידע רגיש או לגלם חשיפות למערכות הגוף המוסדי כולו.

5) הערכת הסיכונים תתייחס למכלול שרשרת האספקה ולסיכונים הנובעים מאופי הפעילות אל מול הגורמים השונים במרחב (מיקור חוץ, נותני שירותים, לקוחות, חו"ל וכו').

6) גוף מוסדי יוכל להסתמך על הערכת סיכונים שביצע ספק מיקור חוץ שהינו גוף מוסדי או תאגיד בנקאי, ובלבד שקיבל את תוצאותיה והניח דעתו בעניין.

7) גוף מוסדי יוכל להסתמך על הערכת סיכונים של ספק מיקור חוץ ובלבד שבוצעה על ידי גורם בלתי תלוי בספק מיקור חוץ וניתנה לגוף המוסדי חוות דעת (לרבות מידע מספק לגבי תהליכי הבקרה ותוצאות הבדיקות שנעשו) כי רמת ההגנה שמיישם ספק מיקור החוץ תואמת את הדרישות מגוף המוסדי.

8) גוף מוסדי ינהל רשימה עדכנית של נכסי המידע ותהליכים הקיימים בו. הרשימה תעודכן לכל הפחות

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

אחת לשנתיים.

9) הערכת הסיכונים תעבור תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בתהליכים עסקיים, בסביבה הטכנולוגית או במתאר הסיכונים, ולכל הפחות אחת ל-36 חודשים.

ב. דיווח וניטור סיכונים

1) הערכת סיכונים תהווה בסיס לתכנית להפחתתם, תשולב בתכנית העבודה ותנחה את הגוף המוסדי בהקצאת משאבים להטמעת אמצעים לניהול סיכוני סייבר.

2) תוצאות הערכת סיכונים ותכנית להפחתתם ידונו בוועדת היגוי יאושרו בה ויוצגו לדירקטוריון. הצגה זו תכלול, לכל הפחות, פירוט סיכונים שיוריים, תכנית הפחתת סיכונים ופירוט הסיכונים המשמעותיים שגוף מוסדי החליט שלא להפחית לרמה מזערית ככל שניתן.

ג. יישום בקרות

בהתאם להערכת הסיכונים וכחלק מהתוכנית להפחתתם יגדיר גוף מוסדי בקרות הגנת סייבר מתאימות ואפקטיביות. על הבקרות להתייחס, למידע, למערכות ולתהליכים בגוף וכן לצדדים שלישיים המספקים שירות לגוף המוסדי.

5. הגנת סייבר של גוף מוסדי

גוף מוסדי יבצע הערכה שנתית של התאמת אמצעי ההגנה למכלול סיכוני הגנת הסייבר שלו. הערכה זו תתחשב בהתפתחויות מתאר האיומים, באופי ההתקפות הנוכחי ובטכנולוגיות הקיימות במטרה להתמודד עם איומים אלה.

להלן יפורטו אמצעי ההגנה שעל גוף מוסדי ליישם:

א. הגנת סייבר, ניטור ובקרה

גוף מוסדי יבסס תמונת מצב עדכנית אודות הגנת הסייבר שלו תוך זיהוי חולשות ואיומים ויפעל לצמצום חשיפות לסיכונים אלו.

1) איסוף מודיעין

א) גוף מוסדי יאסוף וינתח מידע רלוונטי, ממקורות פנימיים וחיצוניים לצורך יצירת תפיסה כוללת ועדכנית של איום הסייבר וחשיפת הגוף המוסדי למול האיום, כבסיס לקבלת החלטות מושכלת, תעדוף של דרכי פעולה, וקיום הגנה אפקטיבית בזמן אמת.

ב) גוף מוסדי יבחן עבודה מול המרכז הלאומי להתמודדות עם איומי סייבר (Cert-il) ולשיתוף הדדי של מידע קיברנטי אופרטיבי עמו.

2) ניטור ובקרת מערכות מידע

א) גוף מוסדי יקיים מערך ניטור ובקרה לקבלת דיווחים בזמן אמת ממערכותיו השונות אודות חשש לאירוע סייבר.

ב) גוף מוסדי יישם נתיב בקרה וניטור של פעולות ושאילתות המתבצעות במערכות המנהלות מידע רגיש על לקוחות וכן במערכות שרמת החשיפה שלהן לביצוע פעילות בלתי מורשה הינה גבוהה (בהתאם להערכת הסיכונים של הגוף), במטרה לאפשר התחקות אחר פירוט הרישום לצורך ביקורת, זיהוי של פעילות בלתי מורשה, תחקור לאחר מעשה ומניעת התכחשות.

ג) נתיב הבקרה האמור יתייחס לפעולות ושינויים המבוצעים במערכות וכן לשאילתות וגישה לנתונים ולכל הפחות גישה למידע רגיש. יתועדו גם ניסיונות לביצוע פעולות (לרבות ניסיונות חיבור למערכות, שאילתות ועדכוני נתונים) שלא צלחו.

ד) נתיב בקרה יכלול מידע על מועד ביצוע הפעולה, מקור הפעולה, הגורם שביצע או ניסה לבצעה ועל מי בוצעה הפעולה. במערכות ליבה - לרבות ערך טרום ביצוע הפעולה ולאחריה.

ה) פרק הזמן לשמירת נתיב בקרה יתאים למטרות נתיב הבקרה, ובכל מקרה לא יפחת מ-12 חודשים.

ו) נתיב הבקרה יהיה מוגן מפני מחיקה או שינוי בלתי מורשה.

ז) גוף מוסדי יתבסס על ניתוח מודיעיני בהתאם לאמור בסעיף 1.א.5)א) וישתמש במערכות ותהליכים שיזהו ויתריעו על פעילות המוגדרת אסורה או חשודה. ההתרעות יתוכננו בהתבסס על הגדרת תרחישי איום ובהתאם להערכת הסיכונים.

ח) זיהוי והתרעה בגין אירועים חריגים כאמור בסעיף 2.א.5)ז) יתייחס לפעולות שמקורן מחוץ לגוף או בתוכו, תוך שימת דגש על מערכות תשתית, מערכות אפליקטיביות ומערכות המנוהלות או מאוחסנות מחוץ לגוף.

ט) זיהוי והתרעה של פעולות חריגות שמקורן מחוץ לגוף מוסדי יכול להתבצע על ידי מיקור חוץ בהינתן והוא עומד בדרישות גוף מוסדי לביצוע ניטור ומתריע לגוף מוסדי בעת התגלותם של אירועים חריגים.

י) מנהל הגנת סייבר יתחקר אירועים חריגים. ועדת ההיגוי תדון בממצאי כל אירוע משמעותי, תפיק ממנו לקחים ותעביר המלצותיה למנכ"ל תוך פרק זמן סביר שלא יעלה על שלושה חודשים.

יא) גוף מוסדי יבחן מעת לעת את חוקי הניטור שהוגדרו, תקינותם ואיכות האירועים שמתקבלים, ולכל הפחות אחת לשנה.

3) מוכנות לאירועים

א) גוף מוסדי ימפה את גורמי האיום ויפעל להבטחת יכולת מוכנות, התגוננות ושרידות בפני התקפות.

ב) גוף מוסדי יגדיר תכנית היערכות וניהול אירועי סייבר, בהתאם להערכת סיכונים ולניתוח תרחישי קיצון (כגון: גישה לא מורשית לנכסי הגוף, זליגת מידע, התחזות, נוזקות, הונאה, מניעת שירות וכדומה).

ג) התכנית תכלול את השלבים הבאים:

(1) גילוי - גילוי וזיהוי השלב בו נמצא האירוע תוך פירוט שלבי פעולה (בידוד, חקירה, איסוף ראיות, הסקת מסקנות וכדומה).

(2) הערכת מצב - בירור וניתוח אירוע הסייבר ובחינת דרכי פעולה להתמודדות עם האירוע.

(3) הכלה ובלימה - השגת שליטה על האירוע ועצירת החמרתו.

(4) התאוששות - הכרעת האירוע תוך מזעור הנזק שנגרם.

(5) השבה לשגרה - חזרה לפעילות מלאה של הגוף המוסדי לאחר תיקון כל נזק שנגרם.

ד) בנוסף, התכנית תפרט לכל הפחות, את הבאים:

(1) אופן תגובה ודרכי פעולה של הגוף, בהתייחס לתרחישים שונים, את אופן יישומן ואת הגורמים האחראים על הפעלתן.

(2) התקשרות עם גורמים פנימיים וחיצוניים, ובכלל לקוחות, בהתאם לתרחישים שונים.

(3) מתכונת ותדירות דיווח על אירועים. לרבות, גורם מדווח, נמען הדיווח וזמן התגובה הסביר לדיווח.

ה) התכנית תעודכן על בסיס שנתי, בהתאם להערכת סיכונים מעודכנת, ותכלול התייחסות גם לעובדים חדשים ולמיקור חוץ.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ו) גוף מוסדי יגדיר תכנית התאוששות ויעדי התאוששות מאירוע סייבר עד לתפקוד מלא בעת חזרה לשגרה, תוך התייחסות לאיומי הייחוס, תרחישי הייחוס, יעדי השירות בחירום שקבע לעצמו ויעדי השירות שהוגדרו כאמור בחוזר "ניהול המשכיות עסקית בגופים מוסדיים" 2013-9-11 ובכל חוזר אחר שיבוא במקומו.

ז) גוף מוסדי יקיים, לכל הפחות, אחת לשנה תרגול של כלל המערכים הרלוונטיים במטרה להכין אותו להפעלת התוכניות שהוזכרו לעיל ולשיפורן בהתאם ללקחי תרגולים שבוצעו.

ח) גוף מוסדי יקים צוות תגובה להתמודדות עם אירועי סייבר, שיערוך תרגול אירוע אמת אחת לשנה, תוך שימוש במערכות ותשתיות הגוף המוסדי.

ט) גוף מוסדי יקבע מנגנון דיווח על אירועי סייבר שיהיה נגיש לעובדים.

י) מנהל הגנת סייבר ידווח לוועדת ההיגוי דוח המסכם אודות כלל ניסיונות התקיפה ואירועי סייבר שהתרחשו (לרבות כאלה שלא הובילו לפגיעה חמורה), ההחלטות והפעולות שבוצעו, אחת לרבעון.

יא) גוף מוסדי ידווח בהקדם האפשרי לדירקטוריון הגוף המוסדי ולממונה על שוק ההון, ביטוח וחיסכון על כל אירוע סייבר משמעותי שכתוצאה ממנו, באופן ישיר או עקיף:

(1) נפגעו או הושבתו מערכות ייצור המכילות מידע רגיש למשך של יותר מ-3 שעות.

(2) יש אינדיקציות לכך שמידע רגיש של לקוחות הגוף המוסדי או עובדיו נחשף או דלף.

ב. ביצוע סקרים

1) סקרים ומבחני חדירה

א) גוף מוסדי יישם כחלק מתכנית העבודה הרב-שנתית, סקרים ומבחני חדירה המכסים את המערכות והתהליכים הארגוניים.

ב) הסקרים והמבחנים יבחנו תאימות מערכות ותהליכים למדיניות ולנהלי סיכוני סייבר של הגוף, הן ברמת בדיקת קיום בקרות להגנת סייבר והתאמתן והן ברמת בדיקת אפקטיביות הבקרות.

ג) הסקרים יכללו ממצאים והמלצות.

ד) תכנית העבודה לביצוע הסקרים והמבחנים תיישם את הנושאים הבאים, בהתאם להערכת הסיכונים:

(1) כיסוי של כל רמות האבטחה של התהליכים והמערכות (ניתן גם באופן רוחבי), לרבות: הגנות פיסיות וסביבתיות, הגנות תשתיתיות הכוללות אחסון, מערכות הפעלה, רשתות, בסיסי נתונים, רכיבי Middleware וכדומה, הגנות אפליקטיביות, הגנות ברמת הלוגיקה העסקית המיושמת במערכת וכן התהליכים הסובבים את המערכת כגון ניהול משתמשים והרשאות, תהליכי גיבוי, ניטור וכדומה.

(2) ביצוע מבחני חדירה תקופתיים הכוללים: מבחן המדמה ניסיון תקיפה מרשתות חיצוניות (כגון רשת האינטרנט, חיבור לספקים או שותפים עסקיים), בדיקות הנדסה חברתית, התחזות ופישינג, לכל הפחות אחת לשנה.

(3) ביצוע סריקת חשיפות אבטחת מידע (Vulnerability Scan) תקופתית לכל הפחות אחת לרבעון (בגוף מוסדי בעל היקף פעילות נמוך אחת לשנה), לזיהוי חשיפות אבטחת מידע טכנולוגיות במערכות הגוף. הסריקות תתייחסנה לחשיפות הנובעות מחיבור מערכות הגוף לרשתות חיצוניות ("סריקה חיצונית") ולחשיפות הנובעות מניסיונות תקיפה מתוך רשת הגוף ("סריקה פנימית").

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

(4) תדירות ביצוע סקרים תיקבע בהתאם למידת החשיפה של המערכת לאיומים, רגישות המידע המנוהל במערכת ושינויים שבוצעו במערכת או בסביבתה.

(5) תדירות ביצוע סקרים למערכות שיש אליהן גישה מרשת ציבורית לא תפחת מאחת ל-18 חודשים, עבור מערכות שאין אליהן גישה מרשת ציבורית לא תפחת מאחת ל-36 חודשים. ועבור מערכות שאין אליהן גישה מרשת ציבורית ולגביהן נקבע סיכון נמוך בהערכת הסיכונים, לא תפחת מאחת ל-48 חודשים.

(6) על אף האמור לעיל, טרם הטמעת שינוי משמעותי במערכת שהוערכה כבעלת סיכון גבוה, או בסביבתה הטכנולוגית, יבוצע סקר לבחינת תאימותה למדיניות ולנהלי סיכוני סייבר של הגוף המוסדי.

ה) סקרים, מבחני חדירה וסריקת חשיפות אבטחת מידע יבוצעו על ידי גורם מקצועי, עצמאי, חיצוני ובלתי תלוי שאינו מעורב בפיתוח והטמעת מערכות בגוף.

ו) גוף מוסדי יגדיר תכנית לביצוע סקרים אצל ספקי מיקור חוץ המאחסנים או מעבדים נתונים של הגוף המוסדי. רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון, ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות הגנת סייבר ולזהות חשיפות לסיכונים אלו. סקרים אלו יבוצעו בתדירות המותאמת לרמת הסיכון ולקצב עדכון התהליכים ומערכות הספק, ולכל הפחות אחת ל-36 חודשים. יתאפשר שימוש בסקרים שיזם ספק מיקור החוץ בהינתן והוא עומד בדרישות חוזר זה לביצוע סקרים ובוצע על ידי גורם בלתי תלוי.

2) טיפול בממצאי סקרים ומבחני חדירה

א) גוף מוסדי יגדיר תהליך שוטף לטיפול בחשיפות אבטחת מידע המתגלות במהלך סקרים ומבחנים, וליישום ההמלצות לטיפול בחשיפות אלו.

ב) תמצית ממצאי סקרים ומבחנים תוצג בוועדת ההיגוי.

ג) במקרים בהם חשיפות בסיכון גבוה לא טופלו במהלך שישה חודשים מעת ביצוע הסקר, מנהל הגנת סייבר יציג בוועדת ההיגוי את הסיבות לאי הטיפול בחשיפות אלו, ואת משמעויותיהן להערכת סיכוני סייבר של הגוף.

ג. אבטחת מערכות, תקשורת ותפעול

כדי ליצור שכבות הגנה על מערכות של גוף מוסדי ועל תהליכיו העסקיים, למנוע התממשות סיכונים, לזהות התממשות סיכונים באופן מהיר, לעצור התפשטות התקפות על מערכות גוף מוסדי ולאפשר שחזור מערכות וצמצום הנזק שנגרם כתוצאה מהתממשות סיכונים, גוף מוסדי ישתמש באמצעים להפחתת סיכונים כדלהלן:

1) אבטחת רשת וגישה מרחוק

א) גוף מוסדי ישתמש באמצעי הגנת סייבר המתאימים לסיכוני גישה מרחוק לרשת הגוף, כגון אמצעי סינון תקשורת ותוכן, אמצעי ניטור הגנת סייבר ותהליכי בקרה.

ב) האמצעים יותאמו לסיכונים ייחודיים לשירותי רשת שונים, כגון דואר אלקטרוני, DNS, שירותי העברת קבצים, שירותי Web ועוד.

ג) גוף מוסדי יישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרגישות הנתונים המנוהלים במערכות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) גוף מוסדי יגדיר אמצעי אבטחה מיוחדים כגון שימוש בהזדהות חזקה, הצפנה מקצה לקצה וניטור מוגבר בגישה מרחוק לרשת הגוף, על גבי תשתית תקשורת ציבורית או מנקודות קצה שאינן מאובטחות דיין.

ה) גוף מוסדי יישם מנגנונים שינטרו ויצמצמו את הסיכונים הנובעים מחיבור התקן זר או התקן בלתי-מאובטח לרשת הגוף.

2) קישוריות גוף מוסדי לרשת האינטרנט

א) גוף מוסדי יצמצם את רמת הגישה של העובדים לרשת האינטרנט למינימום הנדרש, לצורך הגנה מפני סיכוני סייבר.

ב) קישור מערכות גוף מוסדי לרשת האינטרנט יבוצע תוך יישום אמצעי הפרדה מתאימים, שמטרתם למנוע הפעלה של קוד עוין, הכנסה בלתי מבוקרת של קבצים לרשת גוף מוסדי או יצירה של ערוצים חשאיים אל מחוץ לארגון.

ג) גוף מוסדי יבצע הפרדה מוחלטת של רשתות אלחוטיות מרשת הייצור שלו. לחילופין וככל שלא מדובר ברשת אלחוטית לשירות אורחיו, גוף מוסדי יישם מנגנונים מספקים לאבטחת רשתות אלחוטיות, לרבות הצפנה, הזדהות חזקה, מניעת התקפות על הרשת ומניעה של התחברות גורמים או ציודים בלתי מורשים לרשת האלחוטית.

3) הוצאת נתונים אל מחוץ לחצרותיו

א) גוף מוסדי יקבע את האופן שבו תאושר הוצאת נתונים אל מחוץ לחצרותיו, בהתאם לרמת רגישותם.

ב) גוף מוסדי יגדיר את אופן הגנת הסייבר ההכרחי ליישום בתהליך העברת מידע מחוץ לחצרותיו (כגון: הצפנת נתונים, וידוא הגעת נתונים ליעדם וכדומה) בהתאם לרמת רגישות מידע.

4) הצפנה

א) עבור מידע רגיש, גוף מוסדי יישם הצפנה להגנה על חיסיון בתווך התקשורת מחוץ לחצרותיו, יישם טכניקות הצפנה מוכרות שהוכחו כיעילות ויתקף את האפקטיביות של אלה באופן תקופתי.

ב) גוף מוסדי יגדיר נהלים מתאימים ליצירה, עדכון, חידוש, התקנה וביטול של מפתחות הצפנה ככל שרלוונטי לפעילותו.

5) אבטחת תשתיות ומערכות מידע ועדכונן

א) גוף מוסדי ישמור רשימה עדכנית של תשתיות ומערכות מידע לצורך הגנה מפני סיכוני סייבר, ויגדיר תהליכים לשמירת עדכניות רישום זה.

ב) גוף מוסדי יגדיר תהליכי עדכון מבוקרים למערכות ולתשתיות, תוך התייחסות למקוריות קבצי העדכון, בדיקת עדכונים בטרם יישומם, ושמירה על יציבות מערכות בתהליך העדכון.

ג) גוף מוסדי יתייחס לסיכונים הנובעים מחוסר עדכניות או היעדר תמיכה.

ד) גוף מוסדי יישם עדכוני אבטחת מידע שוטפים למערכות ולתשתיות באופן תקופתי.

ה) גוף מוסדי יעקוב באופן תדיר אחר פרסום עדכוני אבטחת מידע למערכותיו ולתשתיותיו, ויישם עדכונים קריטיים בהקדם האפשרי, בהתייחס לרמת חשיפתם לסיכונים הקשורים לעדכונים אלה.

6) אבטחת מערכות קצה

א) גוף מוסדי יישם אמצעי הגנה על מערכות קצה, תוך התחשבות בסיכוני הפעלת קוד עוין וסיכוני חדירה למערכות, תוך ניצול התקנים המחוברים למערכות קצה.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ב) גוף מוסדי יישם הצפנת מידע רגיש במערכות קצה ניידות (כגון מידע הנמצא על מחשבים ניידים, טאבלטים, התקני אחסון ניידים וטלפונים ניידים), במטרה למזער את הסיכון לחשיפתם.

ג) גוף מוסדי ישתמש במערכות בקרה, במטרה לצמצם זליגת נתונים רגישים ממערכות קצה או להגביל את היכולת לשמור מידע רגיש על מערכות קצה.

7) מניעת קוד עוין

א) גוף מוסדי יטמיע אמצעי אבטחה, למניעת חדירה והתפשטות קוד עוין במערכותיו, שיכללו מספר שכבות אבטחה כגון: סינון תקשורת וקבצים נכנסים, סריקת מערכות קבצים, הגנה בזמן אמת על שרתים או תחנות קצה, ומערכות ניטור ומניעה ייעודיות.

ב) גוף מוסדי יעדכן בתדירות גבוהה את אמצעי האבטחה האמורים לעיל, ויגדיר תהליכים לווידוא אפקטיביות אמצעי האבטחה כאמור (כגון: קבלת התרעות על כשל בעדכון קבצי חתימות).

ג) בעת חיבור אמצעי מדיה למערכות מידע יעשה שימוש במנגנוני הגנה אפקטיביים המונעים חדירת קוד עוין, כגון שימוש במערכות "הלבנת קבצים".

8) הגנת סייבר בתהליכי רכש ופיתוח

א) גוף מוסדי יגדיר דרישות הגנה מפני סיכוני סייבר בכל תהליך רכש או פיתוח של מערכות חדשות, ובעת שדרוג מהותי של מערכות מידע קיימות.

ב) שילוב ניהול סיכוני הסייבר בתהליכי פיתוח ותחזוקה יכלול לכל הפחות, את השלבים הבאים:

(1) ייזום ואפיון מערכת: הערכת סיכוני סייבר רלוונטיים והגדרת דרישות הגנה מתאימות בעת ייזום ותכנון מערכת.

(2) פיתוח מערכת: מימוש דרישות סיכוני סייבר המופיעות באפיון מערכת.

(3) בדיקת מערכת: בדיקות במהלך פיתוח ומבחני חדירה, תוך יישום היבטי סיכוני סייבר ולרבות ביצוע סקר אבטחת מידע.

(4) קליטת מערכת: קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי גורמים מוסמכים לכך, תוך וידוא יישום דרישות הגנת סיכוני סייבר.

(5) שינויים במערכת: מנהל הגנת סייבר יקבל דיווח טרם ביצוע שינוי במערכות המידע, ויקבע את רמת המעורבות הנדרשת בהתאם לאופי השינוי, לרגישות נתונים ולהשפעה אפשרית של השינוי על סיכונים וחשיפות המערכת.

ג) הגנת סייבר תוטמע בכל רכיבי המערכת, לרבות: תשתיות, אפליקציה (ככל שרלוונטי), וברמת הלוגיקה העסקית המיושמת במערכת.

ד) מבחני חדירה יבוצעו בטרם הטמעת מערכות בגוף המוסדי.

ה) מבחני חדירה יכללו, לכל הפחות, את הנדרש בעת ביצוע סקר אבטחת מידע, בהתאם לסעיפים 5.ב.1)ד)(1) ו-5.ב.1)ד)(2).

ו) כחלק מן התקשרות לפיתוח מערכת מידע על ידי גורם חיצוני, גוף מוסדי יבטיח כי קוד המקור עבר בדיקה נגד חשיפות אבטחת מידע ואי קיום קוד זדוני.

9) הפרדה בין סביבות ואבטחתן

א) סביבת יצור תופרד מסביבות אחרות, כגון פיתוח ובדיקות.

ב) רשת המשתמשים תופרד מסביבות אחרות וכל גישה מהסביבה תאושר על ידי מערכת להגנה על מפני התקשרויות בלתי רצויות.

ג) הרשאות משתמשים לסביבות ייצור תוגדרנה בנפרד מההרשאות לסביבות האחרות.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

ד) סביבות פיתוח ובדיקות לא יכילו נתונים אמיתיים, אלא אם רמת הגנת הסייבר המיושמת בסביבות אלו הינה בהתאם לרמת ההגנה המיושמת בסביבת הייצור.

ה) העברת נתונים מסביבת ייצור לסביבה אחרת תתבצע בהתאם להנחיות מנהל הגנת סייבר.

ו) העברת מערכות ונתונים מסביבות פיתוח ובדיקות לסביבת ייצור תיערך בצורה מבוקרת, בהתאם לנהלים, כדי למנוע פגיעה בנתונים בסביבת הייצור.

ד. ניהול משתמשים והרשאות

1) ניהול משתמשים

א) גוף מוסדי יגדיר נהלים המתייחסים לתהליכים שונים במחזור חיים של ניהול חשבונות משתמש במערכות מידע של הגוף, החל מיצירת חשבון משתמש ואופן אישורו, ועד לאופן נעילת החשבון בתום העסקה.

ב) תינתן התייחסות מיוחדת ליצירת חשבונות משתמשים עבור ספקים חיצוניים, עובדי מיקור חוץ, ועובדים זמניים, לרבות הגדרת אופן אישור חשבונות אלה, הגבלת השימוש בהם והמעקב אחר ביטולם בתום תקופת העסקה או בתום הפרויקט.

ג) חשבון משתמש ישויך לעובד מסוים, ותוגדר אחריותו של העובד על חשבון זה ועל הפעולות המבוצעות במערכות גוף מוסדי באמצעות חשבון זה.

ד) ככלל, יעשה שימוש בחשבונות משתמש אישיים. עם זאת, במקרים בהם יש צורך בקיום חשבונות שאינם אישיים, כגון כאלה המיועדים לשימוש על ידי תהליך ממוכן, יוגדרו תהליכים מיוחדים לשמירה על סודיות אמצעי ההזדהות של החשבון, להגבלת השימוש בו בכל הניתן ויוגדר גורם האחראי על החשבון. בנוסף, תוגדר מדיניות ניהול סיסמאות סדירה במשתמשים אפליקטיביים.

ה) גוף מוסדי יגדיר תהליכי סקירה תקופתיים ומתועדים שמטרתם לוודא את הצורך בקיום חשבונות המשתמשים. תהליכי הסקירה לכלל החשבונות, יבוצעו לכל הפחות אחת לשנה.

ו) גוף מוסדי יגדיר את אופן נעילת חשבון משתמש במקרה של אי שימוש בחשבון במשך תקופה ממושכת, ואת תהליך אישור שחרור נעילה זו.

2) סיסמאות ואמצעי הזדהות

א) גוף מוסדי יגדיר אופן הזדהות למערכות מידע, באופן המתאים לרמת רגישות המידע המנוהל במערכת ולסיכונים השונים בתהליך ההזדהות.

ב) גוף מוסדי יגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון מסירת אמצעי הזדהות באופן מאובטח למשתמש לאחר זיהויו, שמירה על סודיות הסיסמה והחלפת סיסמה ראשונית על ידי המשתמש.

ג) יש לאמת זהות משתמש כאשר נמסרת לעובד סיסמה ראשונית למערכת. המשתמש יחויב לשנותה בהתחברות הראשונה למערכת. תוקף הסיסמה הראשונית ייקבע למינימום אפשרי, בהתאם לאופי השימוש בחשבון ולא יעלה על 14 ימים.

ד) סיסמאות או אמצעי הזדהות אחרים לא יישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.

ה) גוף מוסדי יקבע את חוזק אמצעי ההזדהות, כגון הצורך בסיסמה חד-פעמית או מורכבות הסיסמה בהתאם להערכת הסיכונים. גוף מוסדי יגדיר אמצעי בקרה על מערך ההזדהות, כגון

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

נעילת חשבון משתמש לאחר ניסיונות גישה כושלים או אי שימוש ממושך בחשבון, החלפה תקופתית של סיסמה ובקרה על מורכבותה.

3) ניהול הרשאות ובקרת גישה

א) גוף מוסדי יגדיר תהליכים מתועדים למתן הרשאות גישה למערכות ושירותים, לרבות: אחריות גורמים עסקיים על אישור הרשאות למערכות עסקיות, התאמת הרשאות לצרכי תפקיד, רמת הסיכון מהרשאות, שינוי הרשאות בעת שינוי תפקיד וביטול הרשאות בעת סיום העסקה.

ב) מתן הרשאות גישה יתבצע על בסיס מינימום הרשאות נדרשות בהתאם ל"צורך לדעת ולבצע".

ג) גוף מוסדי יגדיר תהליכי סקירה תקופתיים, שמטרתם לוודא את הצורך בקיום הרשאות משתמשים. תהליכי הסקירה לכלל ההרשאות, יבוצעו לכל הפחות אחת לשנה.

ד) תהליכי סקירה תקופתיים של חשבונות ספקים חיצוניים, עובדי מיקור חוץ ועובדים זמניים יבוצעו בתדירות גבוהה יותר.

ה. מיקור חוץ (OUTSOURCING)

בהמשך לחוזר מיקור חוץ בגופים מוסדיים 2013-9-16 וכל חוזר אחר שיבוא במקומו, גוף מוסדי ייישם את ההוראות הבאות הנוגעות להגנת סייבר בעת השימוש במיקור חוץ:

1) דרישות הגנת סייבר בהסכמי מיקור חוץ

א) גוף מוסדי יגדיר נוהל לדרישות הגנת סייבר ביחס לסיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. נוהל זה ייושם בעת התקשרות עם גורם מיקור חוץ חדש.

ב) במסגרת הסכם התקשרות עם קבלת שירותי מיקור חוץ:

(1) יאסר על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

(2) בעת הצורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים לצורך מתן השירות, ולא שכפול כלל בסיס הנתונים.

(3) תיבחן דרישה לעמידה בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

ג) תחולת סעיף זה לגבי הסכמי התקשרות קיימים תהיה במועד חידושם.

2) שירות למערכות גוף מוסדי על ידי נותן שירות מיקור חוץ

אספקה של שירותי תחזוקה מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ, תתבצע בתנאים הבאים:

א) נותן שירות מיקור חוץ יקבל אישור פוזיטיבי להתחברות, לפני תחילת עבודתו. מנהל הגנת סייבר יקבע מי בעל הסמכות לאשר התחברות מסוג זה.

ב) גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ ובתיאום מראש עם הגוף המוסדי לאופן ההתקשרות ותדירותה.

ג) גישה מרחוק תתאפשר לזמן מוגבל על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.

ד) גוף מוסדי ייישם הזדהות חזקה בכל גישה מרחוק של נותן שירות מיקור חוץ.

ה) גוף מוסדי ייישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

ו) גוף מוסדי ינטר כל פעילות מהותית שבוצעה בגישה מרחוק.

ז) חשיפת נותן שירות מיקור חוץ למידע אודות לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

3) שירותי מחשוב ענן

שימוש בשירותי מחשוב ענן כפוף להנחיות לעניין מיקור חוץ, ולרבות:

א) בטרם הפעלת שימוש במערכות מבוססות ענן, על גוף מוסדי לבצע הערכת סיכונים ייעודית ולדון בנושא סיכונים אפשריים בוועדת ההיגוי.

ב) גוף מוסדי לא יאחסן מידע רגיש או נתוני לקוחות בענן מחוץ לגבולות מדינת ישראל, אלא אם בדק ווידא שספק הענן מקיים את רמת ההגנה בהתאם לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס״א-2001 ולדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

ג) בשירותי מחשוב ענן מחוץ לגבולות מדינת ישראל, מידע רגיש יוצפן, גם אם התשתית הינה ייעודית.

ד) גישה לנתונים בענן תבוצע דרך כתובות מורשות בלבד.

ה) במקרים בהם נתוני גוף מוסדי מאוחסנים במערכת שאינה לשימושו הבלעדי של גוף מוסדי (Multi-tenant), יעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה, במטרה למנוע חשיפה של מידע רגיש או נתוני לקוחות לגורמים שאינם מורשים.

ו) גוף מוסדי יכלול בהסכם ההתקשרות עם ספק מחשוב הענן, יכולת שליטה ובקרה שלו על הספק וכן אפשרות חד צדדית להפסקת השימוש בשירותי ספק מחשוב הענן תוך מחיקת המידע ממערכותיו והתחייבותו שלא ניתן לאחזר מידע זה במערכותיו.

ו. אבטחה פיסית וסביבתית

1) אזורים מאובטחים

א) בקרות אבטחה פיסיות יתייחסו למכלול הסיכונים הפיסיים והסביבתיים.

ב) גוף מוסדי יחלק את סביבת העבודה לאזורים מאובטחים לפי רמת רגישות המידע אליו ניתן לגשת מאזורים אלו.

ג) גוף מוסדי יישם מעגלים של בקרות גישה פיסית. מעגלים אלו יכללו בקרות מונעות, כגון דלתות נעולות ושערים אלקטרוניים ובקרות מגלות, כגון מצלמות ומערכות אזעקה. רמת הבקרה הנדרשת תותאם לרמת רגישות המידע אליו ניתן לגשת מאזורים אלה.

ד) גוף מוסדי יאפשר גישה לאזורי העבודה בהתאם לצורך, וימנע בהקדם האפשרי את הגישה לאזורים אלה כאשר אין עוד צורך בגישה זו, לרבות בעת שינוי תפקיד או סיום ההעסקה.

ה) על בקרת הגישה באזורים המוגדרים ברגישות גבוהה לכלול לפחות שער כניסה אחד הנפתח על ידי אמצעי זיהוי חזק, כגון אמצעי ביומטרי או כרטיס חכם.

ו) גופים מוסדיים, המעניקים שירותי קבלת קהל במשרדיהם, יפרידו בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בגוף. לא יתאפשר לגורם, שאינו מורשה, להסתובב במשרדי גוף מוסדי ללא פיקוח.

ז) אזורים ציבוריים המכילים מידע רגיש ימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע.

2) אבטחת ציוד ונייררת

רח׳ קפלן 1, ירושלים 9103002 ת.ד. 3100 טל׳ 02-5317111 פקס׳ 02-5695342
www.mof.gov.il

א) הוצאת ציוד המכיל מידע רגיש מאחד ממעגלי האזורים המאובטחים תיעשה בהתאם להערכת סיכונים.

ב) ציוד המיועד להשמדה או תחזוקה או הנמסר אל גורם מחוץ לגוף לא יכיל מידע רגיש הניתן לשחזור שאינו מוצפן. בטרם הוצאה של מערכות מחשב מחוץ לגוף לצורך תחזוקה, תבוצע מחיקת נתונים באופן המונע אפשרות שחזור מידע.

ג) גוף מוסדי יבצע השמדה של ציוד רגיש (פיסי או דיגיטלי) שאין בו שימוש ויגדיר את אופן הטיפול והשמירה עד להשמדתם.

ז. הגנת סייבר במשאבי אנוש וגיוס עובדים

1) הגנת סייבר בתהליך גיוס עובדים

א) עבור משרות שיוגדרו כרגישות על ידי מנהל הגנת סייבר (כגון כאלה המאפשרות גישה למידע רגיש או שיש להן הרשאות העלולות לסכן את הגוף המוסדי), יבוצעו בדיקות לבחינת אמינות המועמדים.

ב) חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי סיכוני סייבר, וילווה בהצהרת סודיות.

ג) חוזה של גוף מוסדי עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ, יכלול התייחסות לסעיפים לעיל.

2) הגנת סייבר בעת מעבר תפקיד או סיום העסקת עובדים

א) לעובדים (לרבות עובדים במיקור חוץ ועובדי קבלן) העוברים תפקיד או מסיימים את העסקתם ייחסמו הרשאות הגישה למידע שאינם צריכים עוד לביצוע תפקידם ובסיום העסקה לא יישארו נכסי מידע של גוף מוסדי בידי העובד.

ב) גוף מוסדי יגדיר בקרות הגנת סייבר נוספות המתייחסות לתקופת הזמן שבין החלטה על מעבר תפקיד או סיום העסקה של עובד ובין ביטול הרשאות הגישה שלו, כגון מעקב מוגבר של מנהל הגנת סייבר אחר בקשות של העובד להרשאות או פעולות חריגות שמבוצעות על ידו.

3) מודעות והדרכה

א) גוף מוסדי יגדיר תכנית להעלאת רמת מודעות של עובדים לסיכוני סייבר (בסעיף זה: **"התכנית"**).

ב) התכנית תשולב במערך הדרכה של גוף מוסדי ותכלול התייחסות לאוכלוסיות העובדים השונות, לרבות מיקור חוץ.

ג) התכנית תגדיר הדרכות תקופתיות לעובדים לפי סוג התפקיד ובמהלך התפקיד ותתייחס להדרכה הנדרשת בעת קבלת עובדים או בעת מעבר לתפקיד חדש.

ד) התכנית תפעל להשגת המטרות הבאות:

(1) העלאת רמת הידע לגבי סיכוני סייבר שגוף מוסדי חשוף אליהם והנגזרות מאופי התפקיד.

(2) העלאת המודעות הארגונית נדרשת כדי לזהות ולהגיב לסיכונים הנובעים מאופי תפקיד העובדים, כגון סיכוני "הנדסה חברתית".

(3) הטמעת נהלי הגנת סייבר של גוף מוסדי תוך הדרכת עובדים באשר לנהלים הרלוונטיים להגנת סייבר במסגרת תפקידם.

6. אבטחת ערוצי קשר עם לקוחות

א. אבטחת ערוצי תקשורת מבוססי אינטרנט

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342

www.mof.gov.il

1) גוף מוסדי ימפה את ערוצי התקשורת שלו עם לקוחותיו (בסעיף זה לרבות צדדים שלישיים) ויישם מערך בקרות כנגד סיכוני סייבר.

2) מערך הבקרות בערוצי התקשורת מבוססי אינטרנט, יכלול:

א) הצפנת ערוצי התקשורת למניעת האזנה או התערבות.

ב) אמצעי הגנה למזעור סיכונים הנובעים מרמת אבטחה לקויה של ציוד הקצה של לקוחות.

ג) ניטור ייעודי לזיהוי התקפות על ערוצי תקשורת עם לקוחות, כגון: ניסיונות התחזות, התקפות שונות על מנגנוני אימות זהות לקוח (אותנטיקציה), התקפות "הנדסה חברתית", התקפות על מנגנוני שחזור סיסמה וכדומה.

ד) אמצעים מקובלים למניעת התקפות על ערוצים אלה כגון ניחוש שמות משתמשים (user harvesting), ניחוש סיסמאות (Brute force), מניעת שירות באמצעות נעילת חשבונות וכדומה.

3) גוף מוסדי יוודא כי סיכונים שעלולים להיווצר בעת שינויים במערכות מקוונות או בתהליכי הזדהות של לקוחות לשירותים מקוונים, יטופלו באופן מספק, טרם ביצוע השינוי.

ב. רישום מבוטחים/עמיתים לפעילות

1) וידוא זהות בתהליך הרישום

א) גוף מוסדי יוודא זהות לקוח בטרם השלמת רישום לשירותים מקוונים.

ב) וידוא זהות לקוח יעשה באמצעות שימוש בערוץ תקשורת המבוסס על מידע מוקדם שיש לגוף על הלקוח (כגון: משלוח מכתב לכתובת הלקוח שנמסרה לגוף מבעוד מועד, משלוח הודעת SMS למספר טלפון שהלקוח מסר לגוף מבעוד מועד וכדומה).

ג) במקרים בהם לא קיים ערוץ תקשורת המבוסס על מידע מוקדם, ניתן לוודא זהות לקוח באמצעות אוסף פרטי מידע שיש לגוף על הלקוח, ושאינם ידועים לגורם אחר מלבד הלקוח ובלבד שייבחנו סיכונים רלוונטיים (כגון: התחזות) ויושמו מנגנוני אבטחה לצמצומם (כגון: ניטור שמטרתו לזהות ניסיונות התחזות). דוגמאות לפרטי מידע מסוג זה, יכולים להיות: תאריך הנפקת תעודת זהות, פרטים שהלקוח מילא בעבר בשאלון של הגוף המוסדי, פרטים מתוך אמצעי התשלום של הלקוח וכדומה.

2) הסכמה מפורשת של לקוחות בטרם רישום לפעילות

א) רישום לקוח לפעילות בערוצים מקוונים, יחייב קבלת הסכמה מתועדת של הלקוח באמצעות טופס ידני או טופס מקוון או הקלטה או באמצעות חשבונו המקוון של העמית באתר האינטרנט של החברה.

ב) לעמית תינתן הזכות לחזור בו מהסכמתו כאמור.

ג. הזדהות לקוחות לערוצי שירות

1) גוף מוסדי יגדיר את אופן הזדהות הלקוחות לערוצי שירות שונים. אופן ההזדהות יתאים לאופי ערוץ השירות, לרמת הרגישות של המידע, לסוג הפעולות המבוצעות באמצעות הערוץ, ולסיכונים השונים לתהליך ההזדהות, כגון התחזות, הכחשה, האזנה לתווך התקשורת וכדומה. בערוצים מבוססי אינטרנט יעשה שימוש באמצעי הזדהות חזקים או אמצעי הזדהות שאינם קבועים, כגון סיסמאות חד פעמיות הנשלחות בהודעת SMS.

2) גוף מוסדי יגדיר נהלים המתייחסים למסירת אמצעי הזדהות, כגון משלוח סיסמה ראשונית באמצעות דואר לכתובת לקוח, מסרון לנייד הלקוח או באמצעות ערוץ אחר המאפשר מסירת אמצעי ההזדהות ללקוח, וצמצום הסיכון לגניבת או העתקת אמצעי זה בדרך אל הלקוח.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

3) גוף מוסדי יוודא כי לעובדיו אין גישה לאמצעי הזדהות של לקוחות, העלולה לאפשר ניצול לרעה של חשבון לקוח, למעט עובדים מורשים.

4) גוף מוסדי יגדיר נהלים לוודוא חוזק סיסמה, שמירה על סודיותה, החלפת סיסמה ראשונית על ידי המשתמש ותוקף הסיסמה הראשונית.

5) בעת שימוש באמצעי זיהוי קבועים גוף מוסדי יגדיר נהלים המאפשרים ללקוח איפוס סיסמה באמצעים האמורים בסעיף 6.ג.2).

ד. שליחת מידע באמצעים דיגיטליים

1) גוף מוסדי ישלח מידע רגיש ללקוחות באמצעים דיגיטליים, בכפוף לתנאים הבאים:

א) גוף מוסדי יצפין את המידע, כך שיימנע חשיפתו לגורם זר או לשיבושו.

ב) גוף מוסדי יוודא כי ההודעה שנשלחה תקינה ולא התקבל סימן שלא הגיעה ליעדה.

ג) גוף מוסדי ישמור כל מידע תפעולי הנחוץ לצורך בקרה, ניהול ומעקב אחר קיום תנאי שליחת מידע באמצעים אלקטרוניים.

2) גוף מוסדי יספק ללקוחותיו מידע והנחיות שיסייעו להם לנקוט באמצעי זהירות נדרשים לשמירה על פרטיות מידע, וינחה אותם כיצד לנהוג במקרה של חשד לאירוע סייבר.

ה. שיווק מוצרים באמצעים דיגיטליים (ומסחר דיגיטלי)

שיווק מוצרים באמצעים דיגיטליים יתבצע בכפוף לתנאים הבאים:

1) ערוץ תקשורת המשמש את תהליך הרכישה יוצפן באמצעות הצפנה חזקה בהתאם לתקנים המקובלים בשוק, שתבטיח את שלמות המידע וסודיותו, תוך שימוש בתעודת הצפנה (Certificate) חתומה על ידי גוף מוכר ואמין.

2) פרטי אמצעי התשלום של המבוטחים הנשמרים בשרתי החברה, ישמרו בהתאם לתקנים המקובלים בשוק.

3) גוף מוסדי יישם אמצעים למניעת הכחשה, כגון תיעוד בלתי ניתן לעדכון של פרטי ההסכם עם הלקוח, וכן יבקר וינטר את אמצעי המסחר הדיגיטלי במטרה למנוע התחזות ללקוח, הונאה או ניצול לרעה של תהליכי המכירה.

7. אבטחת ערוצי קשר עם גורמים חיצוניים

א. אבטחת ערוצי קשר בין גופים מוסדיים לבין בעלי רישיון

1) לבעלי רישיון שאינם עובדי גוף מוסדי לא תותר גישה ישירה אל מערכות המידע ברשת הפנימית (קישור ישיר ל LAN) של גוף מוסדי, אלא דרך מערכת שער מאובטחת (Secure Gateway), הממוקמת באזור מפורז מחוץ לרשת הפנימית שתיזום את ההתקשרות לרשת הפנימית בשם בעל הרישיון. במקרים בהם בעלי רישיון משתמשים באותה רשת של גוף מוסדי והתקשורת ביניהם אינה עוברת על גבי תווך ציבורי, תותר גישה ישירה אל מערכות המידע ברשת הפנימית.

2) בכל חיבור של בעלי רישיון למערכות תפעוליות של גוף מוסדי, על הגוף להבטיח בקרת גישה מאובטחת. בקרת הגישה תכלול הזדהות חזקה, הצפנת תווך התקשורת מקצה לקצה, חלוקת הרשאות על בסיס "הצורך לדעת ולבצע" ויישום בקרות למניעה ואיתור של אירועים חריגים.

3) לכל עובד במשרדי בעלי הרישיון יהיה זיהוי חד ערכי מול מערכות המידע של הגוף המוסדי.

4) גוף המוסדי יגדיר לכל עובד במשרדי בעלי הרישיון הרשאות גישה למערכות השונות על פי צורך בלבד. הרשאות אלו יותאמו לסוג ולתוקף ההתקשרות עמו.

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

5) גוף מוסדי יבחן את הרשאות הגישה הניתנות לכל בעל רישיון מעת לעת, ולכל הפחות אחת לשנה.

6) כל גישה של בעלי רישיון למערכות גוף מוסדי תבוצע על תווך תקשורת מוצפן מקצה לקצה.

7) לא יותר שימוש בתוכנות השתלטות על מחשבי בעלי רישיון באופן העלול לגרום לחשיפת מידע רגיש בין גוף מוסדי למשנהו.

8) גוף מוסדי יגדיר כללים מתועדים בתחום ניהול סיכוני הסייבר אותם יישמו בעלי רישיון. שיתוף פעולה בין גוף מוסדי לבין בעל רישיון יותנה בעמידה בכללים שהוגדרו.

9) תיבחן דרישה מבעלי רישיון לעמוד בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

ב. אבטחת ערוצי קשר בין גופים מוסדיים

בעת יצירת ערוצי העברת מידע בין גופים מוסדיים תיושמנה בקרות הגנת סייבר הכוללות הצפנת תווך התקשורת והנתונים מקצה לקצה, אפשרות מעקב אחר הגעת הנתונים ליעדם והגבלת הגישה לנתונים על בסיס "הצורך לדעת", למעט במקרים בהם גופים מוסדיים משתמשים באותה רשת והתקשורת ביניהם אינה עוברת על גבי תווך ציבורי.

8. החלת ההוראה

א. תחולה

הוראות חוזר זה יחולו על כל הגופים המוסדיים.

ב. תחילה

1) מועד תחילתו של חוזר זה ב- 2 באפריל 2017.

2) על אף האמור בסעיף קטן 1), מועד תחילתם של סעיפים 2.א.5), 6, ו- 7.א. (ניטור ובקרת מערכות מידע, אבטחת ערוצי קשר עם לקוחות ואבטחת ערוצי קשר בין גופים מוסדיים לבין בעלי רישיון) יהיה ב-1 באוקטובר 2017.

ג. ביטול תקפות

חוזר גופים מוסדיים 2006-9-6, "הוראה לניהול סיכוני אבטחת מידע של הגופים המוסדיים" - בטל.

דורית סלינגר

הממונה על שוק ההון ביטוח וחסכון

רח' קפלן 1, ירושלים 9103002 ת.ד. 3100 טל' 02-5317111 פקס' 02-5695342
www.mof.gov.il

52% 12:58

Shirbit

11:11, 01 דצמ'

6 ס

לקוח/ה נכבד/ה,
ממידע שנתקבל בחברה ומבדיקות שנערכו קיים חשד לאירוע סייבר כנגד החברה, במסגרתו הוצאו מהחברה מסמכי ביטוח. נציין שאין בנתונים שהוצאו מידע שעלול לגרום נזק למבוטחינו. החברה נקטה ותמשיך לנקוט בכל האמצעים הדרושים כדי לטפל באירוע ולהבטיח מניעה של השנות אירועים שכאלה בעתיד. האירוע עודנו בטיפול בשיתוף מערך הסייבר ורשות שוק ההון, בטוח וחיסכון.
בכבוד רב,
שירביט חברה לביטוח בע"מ

העתק טקסט
שתף