Dr. Dan Hay, Adv. & Notary
Daniel Efrati, Adv.
Ben Baharav, Adv.
Tomer Arad, Adv.
Idan Zur, Adv.
Adi Goshen, Adv., M.Sc. PA.
Naomi Helfand, M.Sc. PA.
Kfir Wittman, Adv.
Sapir Gueta, Adv.
Gavriel Labaton, Adv.
Hagar Amit, Adv.
Yair Ben Shlomo, Adv.
Gilad Malki, Adv.
Inbal Dror, Adv.
Liam Hazan, Adv.
Roei Dayan, Adv.
Tomer Finkelstein, Adv.
Adi Teper Averbuch, Adv.
Nir Dekel, Adv.
Sahar Saban, Adv.
Nirel Ben Yashar, Adv.
Naomi Assia, Adv – of counsel.

ד"ר דן חי, עו"ד ונוטריון
דניאל אפרתי, עו"ד
בן בהרב, עו"ד
תומר ארד, עו"ד
עידן צור עו"ד
עדי גושן, עו"ד, עו"פ
נעמי הלפנד, עו"פ
כפיר ויטמן, עו"ד
ספיר גואטה, עו"ד
גבריאל לבטון, עו"ד
הגר עמית, עו"ד
יאיר בן שלמה, עו"ד
גילעד מלכי, עו"ד
ענבל דרור, עו"ד
ליאם חזן, עו"ד
רועי דיין, עו"ד
תומר פינקלשטיין, עו"ד
עדי טפר אברבוך, עו"ד
ניר דקל, עו"ד
סהר סבן, עו"ד
ניראל בן ישר, עו"ד
נעמי אסיא, עו"ד – יועצת בכירה

23 נובמבר, 2025

לכבוד
<u>הסתדרות המורים בישראל</u>

הנדון: שימוש במידע מתוך מאגר המידע של ההסתדרות
<u>והעברתו לסיעות המתמודדות בבחירות למוסדות ההסתדרות</u>

1. <u>מבוא</u>:

1.1. ביום 17 בפברואר 2026, יתקיימו בחירות (להלן "**הבחירות**") במוסדות הסתדרות המורים בישראל (להלן "**ההסתדרות**").

1.2. לקראת הבחירות, נתבקשנו לבחון עבורכם את סוגיית העברת המידע המצוי במאגר המידע של ההסתדרות (כהגדרתו להלן) בידי ההסתדרות לסיעות המתמודדות בבחירות ולבחון את הפעולות הדרושות לשם שימוש נכון במידע זה. זאת בראי חוק הגנת הפרטיות, התשמ"א-1981 (להלן "**החוק**"), ובכלל זה תיקון 13 לחוק שנכנס לתוקפו באוגוסט 2025 (להלן "**תיקון 13**"), הנחיות הרשות להגנת הפרטיות (להלן "**הרשות**"), אשר בראשה עומד ראש הרשות להגנת הפרטיות (להלן "**ראש הרשות**") ואשר אמונה על אכיפת פרק ב' לחוק העוסק בהגנה על הפרטיות במאגרי המידע, תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן "**תקנות אבטחת המידע**") וכל הוראת חוק רלבנטית אחרת.

להלן חוות דעתנו.

2. רקע משפטי

2.1. חוק הגנת הפרטיות הוא המסדיר את דרכי ניהול והחזקת המידע האישי בישראל וקובע מספר עקרונות בהם ניתן לעשות שימוש במידע האישי, כך שלא יהווה הפרה לפי חוק זה. המידע הנאסף על-ידי גורמים שונים, קיבל תשומת לב מיוחדת עם כניסתן לתוקף של תקנות אבטחת המידע, בתחילת חודש מאי 2018 אשר קבעו הסדרים מפורטים באשר לניהול מאגרי מידע והגנה עליהם, וזאת בכפוף להוראות פרק ב' לחוק. בהמשך לכך, תיקון 13, שנכנס לתוקפו בחודש אוגוסט 2025, הרחיב באופן משמעותי את המסגרת הנורמטיבית החלה על עיבוד מידע אישי בישראל, ובין היתר עיגן את החובה למנות ממונה על הגנת הפרטיות על גופים מסוימים, הרחיב את זכויות נושאי המידע (ובהן זכויות העיון והתיקון), צמצם את חובת הרישום של מאגרי מידע, והעניק סמכויות אכיפה נרחבות לרשות להגנת הפרטיות.

2.2. "מאגר מידע" מוגדר בחוק כאוסף פרטי מידע אישי המעובד באמצעי דיגיטלי, למעט אוספים לשימוש אישי או כאלו הכוללים רק שם, מען ודרכי התקשרות הכוללים פחות מ-100,000 בני אדם.[1]

2.3. "מידע אישי" מוגדר בחוק כך: "נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי". אדם הניתן לזיהוי הינו מי שניתן לזהותו באופן ישיר או עקיף, ובפרט אם ניתן לזהותו על ידי מספר מזהה או על-ידי תכונה אחת לפחות ביחס לזהותו הפיזית, הכלכלית, התרבותית או החברתית.

2.4. "מידע בעל רגישות מיוחדת" מוגדר בחוק כמידע אישי שהטיפול בו עלול לחשוף את נושאו לפגיעה חמורה יותר בפרטיותו, ועל כן הוסדר לגביו מערך חובות מוגבר. במסגרת תיקון 13, נקבעה לראשונה רשימה מפורטת של סוגי מידע הנכללים בגדר הגדרה זו, ובהם מידע על צנעת חייו האישיים של אדם (ובכלל זה נטייתו המינית), מצבו הבריאותי, עברו הפלילי, אמונותיו ודעותיו הפוליטיות, נתונים ביומטריים ועוד. הגדרה זו נועדה לשמש כלי מרכזי בקביעת רמת האבטחה הנדרשת למאגרי מידע בהתאם לתקנות אבטחת מידע, והיא מהווה נדבך מרכזי ברפורמה שנקבעה בתיקון 13.

2.5. ההגדרה של "מאגר מידע" לצורך החוק הינה הגדרה משפטית, לא טכנולוגית. בכלל זה, המידע הרלבנטי להגדרה זו עשוי ויכול להישמר במגוון סוגי מערכות וצורות ניהול משותפות, לרבות מערכות ניהול נתונים מרכזיות (CRM, ERP) ואף מערכות דואר אלקטרוני או גיליונות אלקטרוניים שונים. מערכות המידע השונות מיועדות כדי לתת מענה לעיקרון המצוי בבסיס הוראות פרק ב' לחוק הגנת הפרטיות, והוא הסדרת אופן השימוש במידע המצוי במאגרים ואבטחתו. לפיכך, היכולות לנהל את המידע, בהתאם למטרות שמירתו, הרשאות הגישה אליו והשימוש בו בהתאם לצורך, הן אלו שצריכות לקבוע את אופן הגדרת מאגרי המידע ואת מטרותיהם.

2.6. בתיקון 13 לחוק הורחבה הגדרת "מידע אישי" כך שהיא כוללת כל נתון המתייחס לאדם מזוהה או שניתן לייחסו לאדם שניתן לזהותו. לעניין זה, "אדם הניתן לזיהוי" הוא מי שזיהויו אפשרי במאמץ סביר, בין באופן ישיר ובין בעקיפין, לרבות באמצעות פרט מזהה

[1] סעיף 3 לחוק מגדיר מאגר מידע כך: " "מאגר מידע" – אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי, למעט אחד מאלה: (1) אוסף לשימוש אישי שאינו למטרות עסק; (2) אוסף הכולל רק שם, מען ודרכי התקשרות, לגבי 100,000 בני אדם או פחות, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם;

כגון שם, מספר טלפון, מספר תעודת זהות, נתוני מיקום, כתובת דואר אלקטרוני, או כל נתון אחר המאפשר את זיהויו. מכאן, כי כתובות דואר אלקטרוני באות בגדר נתונים המאפשרים זיהוי של אדם בהתאם לתיקון 13, ובהתאם, אוסף כתובות דואר אלקטרוני מהווה "מאגר מידע" כהגדרתו בחוק.

2.7. על מנת שיוכל להיעשות שימוש במידע המצוי במאגר כך שלא יהווה הפרה, יש לעשות זאת בהתאם להוראות החוק, לכן להגדרת מטרת השימוש במאגר ישנה חשיבות מכרעת. כך, במסגרת הסדרה פנימית של מאגרי המידע שבשליטת החברה באמצעות מסמך הגדרות המאגר, יש לקבוע את מטרות המאגר ולתת לכך תשומת לב מרבית. להגדרה זו חשיבות מיוחדת לאור הוראות סעיף 8(ב) לחוק, הקובע כי "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין". החלק המשלים של חובה זו הוא קבלת ההסכמות ממושאי המידע למטרות המאגר. זאת בהתחשב בהוראת סעיף 2(9) לחוק, הקובעת איסור על "שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה"[2], זאת מבלי להבחין האם המידע מצוי במאגר המידע, אם לאו, והאם המאגר חייב ברישום. שני עקרונות אלה, עקרון "צמידות המטרה" ו"עקרון ההסכמה" מהווים אפוא, עקרונות מנחים.

2.8. הבסיס הראשוני לעקרון ההסכמה, המהווה עקרון יסודי בדיני הגנת הפרטיות לאותה הסכמה הנדרשת ממושאי המידע, נקבע כבר בסעיף 1 לחוק, הקובע כי "*לא יפגע אדם בפרטיות של זולתו ללא הסכמתו* ". כך מקום בו הסכים אדם לפגיעה המוגדרת בפרטיות, לא תהא זו הפרה של החוק. לפי ההגדרה של "הסכמה" בסעיף 3 לחוק, על ההסכמה להיות מדעת ובנוסף לכך הסכמה שהושגה במפורש או מכללא.[3] ככל שמושא המידע מודע למטרות איסוף המידע אודותיו ומסכים למסירתו למטרות אלה, אין צורך בהסכמה נוספת לצורך עשיית פעולות נוספות במידע, כגון עיבוד הנתונים במידע, כל עוד אין בפעולות אלו משום חריגה מהמטרות לשמן הוקם המאגר (קרי, המטרות הרשומות במסמך הגדרות המאגר עבור מאגר שאינו נדרש ברישום, או בפנקס מאגרי המידע עבור מאגר הנדרש ברישום).

2.9. חובת מבקש המידע, בנוסף, הקפדה על קבלת ההסכמה של מושאי המידע למטרה, כלולה גם בסעיף 11 לחוק העוסק באופן איסוף המידע למאגר, ונוגע לאיסוף נתונים באופן ישיר. בהתאם לסעיף, מקום בו המידע המצוי במאגר המידע נאסף על-ידי בעל השליטה במאגר באופן ישיר, חלה עליו החובה להודיע לאדם ממנו נאסף המידע אם חלה עליו חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו ; המטרה אשר לשמה מבוקש המידע ; שמו של בעל השליטה ודרכי ההתקשרות עמו ; למי יימסר המידע ומטרות המסירה וכן על קיומן של זכות העיון וזכות התיקון במידע.

---

[2] הפרשנות המקובלת לצרוף המילים "ענייניו הפרטיים של אדם" שבסעיף 2(9) לחוק, כוללת "כל מידע הקשור לחייו הפרטיים של אותו אדם, לרבות שמו, כתובתו, מספר הטלפון שלו, מקום עבודתו, זהות חבריו, יחסיו עם אשתו ויתר חברי משפחתו וכדומה". [ע"א 439/88 **רשם מאגרי מידע נ' ונטורה ואח'**, פ"ד מח (3) 808, בעמ' 821]. פרשנות מרחיבה זו היא אך משלימה לענייניים שהם פרטיים במובהק, כגון הגדרות המונחים 'מידע' ו'מידע בעל רגישות מיוחדת' בסעיף 3 לחוק.

[3] השינוי בהגדרה כי על ההסכמה להיות "מדעת" נעשה בתיקון מספר 9 לחוק מיום 21.6.2007. בתזכיר הצעת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ו—2005, עמ' 232, בדברי ההסבר להצעה נאמר כי "**התיקון המוצע נועד להבטיח כי ההסכמה הניתנת לפגיעה בפרטיות, תהיה הסכמה מדעת. היינו, שבידי האדם המסכים לפגיעה בפרטיות יהיה מידע, הדרוש לו, באורח סביר, כדי להחליט האם להסכים או לא, והמידע יימסר לו בצורה מובנת.**"

2.10. המשמעות של הוראת סעיף 11 לחוק, הינה כי בעל השליטה במאגר יכול לעשות שימוש במידע שאסף ובלבד, שבין היתר, הודיע לאדם אשר מסר את המידע את הפרטים המופיעים בסעיף 2.8 לעיל במועד מסירת המידע. הסעיף מתייחס לאיסוף נתונים על ידי פנייה ישירה לאדם, כך שבמצב דברים זה אותו אדם ער לכך שנתונים אודותיו נאגרים ומודע למטרת שמירת נתונים אלו. מנוסח סעיף 11 לחוק עולה החלוקה המתבקשת בנוסחי ההסכמה המתקבלים ממושאי המידע, לשני חלקים אשר לגבי כל אחד מהם מתקבלת הסכמה נפרדת: (1) הסכמה שאדם חייב לתת לצורך הפעילות המבוקשת והמידע הנאסף אודותיו לצורך כך (הסכמה שאין חובה להחתים עליה בנפרד בטופס, כאשר כך נאספים הפרטים); (2) הסכמה לצרכים שאינם אינטגרליים לשם קבלת השירות/מוצר המבוקש- ברוב המקרים לצרכים משלימים, כגון דיוור ישיר, שיווק, העברת מידע לצד שלישי וכיו"ב- הסכמה לגביה יש לקבל הסכמה בחתימתו של הלקוח ליד סעיף או פיסקה נפרדים, או בסימון אקטיבי של הסכמה כזו בריבוע המיועד לכך וכד'. כל זאת, כעולה מפרשנות סעיף קטן (1) של סעיף 11 לחוק, הקובע כי יש להבהיר לאדם ממנו נאסף המידע אם חלה עליו חובה חוקית למסור את המידע (חלק ההסכמה הראשון) או שמסירת ההסכמה תלויה ברצונו ובהסכמתו (החלק השני של ההסכמה).

2.11. כאשר מאגר מידע כולל בין מטרותיו מטרה של "דיוור ישיר", אשר נכללת אף בהודעה שקיבל מושא המידע בהתאם לסעיף 11 לחוק ונכלל בנוסח ההסכמה, ניתן לפנות אל מושא מידע זה בדיוור ישיר. הכוונה, בהתאם להגדרה שבסעיף 3 לחוק, ל-"פניה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע". בפניה כזו יש להקפיד על עמידה בהוראות סעיף 17ו (א) לחוק, הכולל את הדרישות שעל הפונה בדיוור ישיר לעמוד בהן, ובין היתר ציון המאגר המשמש בסיס לפנייה, זהות הפונה ומתן האפשרות להימחק מרשימת הדיוור הישיר של המאגר (מקום בו המאגר אינו משמש רק לדיוור ישיר).

2.12. אבטחת מידע ותקנות אבטחת המידע, לפי סעיף 17.(א) לחוק, מוטלת אחריות על אבטחת המידע שבמאגר המידע על בעל שליטה במאגר מידע. לצד הוראת חוק זאת נכנסו לתוקף, כאמור, תקנות אבטחת המידע אשר קובעות הסדר מעודכן, מקיף ומפורט לעניין ההגנה הפיסית והלוגית ביחס למאגרי מידע ולעניין סדרי הניהול וכללי העבודה במאגרי מידע ובקשר אליהם.[4] ההסדר הקבוע בתקנות כולל הן מנגנונים חיצוניים והן כלים פנים ארגוניים, אשר ממחישים את החובות והאחריות המוטלת על ארגונים המחזיקים במידע בתחום אבטחת מידע אישי, ומטרתו להנחיל עקרונות אבטחת מידע עבור כל ארגון אשר ברשותו מאגרי מידע, ציבורי ופרטי כאחד.

2.13. ההסדרים המוצעים בהסדר המוטמע בתקנות האבטחה נחלקים לשלושה רבדים- הרובד הראשון קובע, כי על בעל השליטה במאגר המידע לקבוע מהו המידע המוגן והסיכונים הקשורים אליו. במסגרת הרובד השני, נדרש הארגון לקבוע נהלים ברורים ומפורטים בנוגע לאבטחת המידע. בתוך כך, בין היתר, בעת פגיעה בפרטיות במאגר מידע, מצבו של ארגון אשר נקט באמצעים סבירים למניעת הפגיעה כאמור יהא שונה ממצבו של ארגון אשר משך ידיו

[4] עמ' 1022 לקובץ התקנות ברשומות.

מהפעולות הנדרשות בהתאם לתקנות. לבסוף, הרובד השלישי כולל הוראות מהותיות ביחס לניהול אבטחת מידע.

2.14. בהיבט האחריות הארגונית, התקנות הינן מודולריות ומחילות חובות ברמה הולכת וגדלה ככל שפעילות עיבוד המידע בארגון משמעותית יותר, ובהתאם לרמת האבטחה הנדרשת למאגר כהגדרתו לאחר תיקון 13) הווה אומר, ככל שמדובר במידע רגיש יותר, או מאגר אודות יותר אנשים, או ככל שיותר גורמים בארגון חשופים למידע וניתנת להם הרשאת גישה אליו, כך, בהתאם, קובעות התקנות חובות ענפות ומחמירות יותר ביחס לניהול ואבטחת מאגר המידע השייך לאותו ארגון.

2.15. ביחס לאמור לעיל, התקנות מגדירות מספר "רמות אבטחה" למאגרים, החל ממאגר המנוהל בידי יחיד, מאגר הנדרש לרמת אבטחה בסיסית, מאגר הנדרש לרמת אבטחה בינונית ומאגר הנדרש לרמת אבטחה גבוהה. התוספת הראשונה לתקנות מפרטת באילו מקרים מאגר יסווג ברמת האבטחת הבינונית וכאשר מאגר עונה להגדרה זו אך יש בו יותר ממאה אלף מושאי מידע או מעל 100 מורשי גישה, הוא יסווג ברמת האבטחה הגבוהה. ככל והמאגר מסווג ברמת אבטחה גבוהה יותר, כך יחולו לגביו הוראות מחמירות יותר בתקנות, בהתאם לאמור בסעיף 21 לתקנות האבטחה.

2.16. כאמור, כאשר מאגר מידע נדרש לרמת אבטחה גבוהה נדרש בעל השליטה במאגר לעמוד בהוראות תקנות האבטחה המחמירות ביותר, כפי שנקבע בתקנה 21 לתקנות האבטחה. התקנות קובעות שורה של הוראות ונהלים בהם מחויב בעל השליטה במאגר ובכלל זה הממונה על אבטחת המידע של המאגר. בין היתר ניתן למצוא הוראות בדבר: נהלי תיעוד ובקרה, נהלי גיבוי ושחזור, נהלי התמודדות עם אירוע אבטחה, נהלי בקרות גישה, נהלי אבטחה פיזית וסביבתית, וכו'. מלבד זאת, על בעל השליטה במאגר לבצע סקר ניהול סיכונים אחת ל-18 חודשים, ו-"סקר עמידות מערכת" ("Penetration Test") בפני סיכונים פנימיים וחיצונים. ביצוע סקר הסיכונים נדרש מיום הקמת המאגר בראי אבטחת מידע והגנת פרטיות כאחד.

3. <u>רקע עובדתי</u>:

3.1. ההסתדרות היא בעלת השליטה במאגר מידע כהגדרתו בחוק (מאגר מידע "עובדי הוראה"; להלן "**המאגר**"). מטרות המאגר הן: ניהול וייעול הקשר עם עובדי ההוראה; מתן שירותי תמיכה וליווי; צרכים תפעוליים, שיווקיים, מסחריים וסטטיסטיים של ההסתדרות; ניהול סטטוס חברים של עובדי ההוראה; צירוף חברי הוראה חדשים; התאמה אישית של חוויית המשתמש; טיוב והעשרת נתונים; שיפור ממשקי ההזמנה והשירות; יצירת קשר יזום או תגובתי עם עובדי ההוראה; קיום סקרי שביעות רצון, פיקוח ובקרת איכות השירות; מחקר וניתוח מגמות לשם פרסום ושיפור ממשקי ההסתדרות; ביצוע דיוור ישיר; שליחת מסרים פרסומיים ושיווקיים באמצעי המדיה השונים (להלן "**מטרות המאגר**").

3.2. המאגר מכיל למעלה מ-100,000 רשומות (כ-300,000 אנשים) ומספר מורשי הגישה למידע שבמאגר עולה על 100, ועומד על כ-200. לכן, רמת האבטחה החלה עליו לפי תקנות אבטחת המידע היא רמת האבטחה הגבוהה, שהינה רמת האבטחה המקסימלית.

3.3. בעת הצטרפות חבר חדש לשורות הסתדרות, מאשר המצטרף בחתימה את הסכמתו לנוסח ההסכמה, אשר בין היתר מאפשר כי מידע אישי אודותיו ישמש למטרות ההסתדרות המפורטות מעלה. נוסח ההסכמה מצורף כ**נספח א'** לחוות דעת זו.

3.4. סעיף 17 לתקנון בחירות לסניפים ולוועידות הסתדרות המורים בישראל, אשר מהווה נספח א' לחוקת ההסתדרות, קובע כי האגף לארגון בהסתדרות המורים יפיק פנקס בוחרים, אשר יכיל את שמות בעלי זכות הבחירה ונתונים נוספים כגון תעודות זהות, מקום מגורים וכו' (להלן "**פנקס הבוחרים**").

3.5. במסגרת הליך הבחירות בהסתדרות עתידה להתבצע, כפי שיובהר להלן, העברת פנקס הבוחרים לידי הסיעות ובמסגרת כך העברת מידע מהמאגר אליהן האמור לכלול, בין היתר, את שמותיהם של חברי הסתדרות המורים וכן פרטי התקשרות עמם כגון טלפון, דוא"ל וכתובת (להלן "**פרטי ההתקשרות**").

3.6. האמור בס"ק 3.4 לעיל עולה עם קביעת בית הדין של ההסתדרות, בהחלטה מיום 28.1.2015 (בתיק 30300/9 סיעת "נחל" בהסתדרות המורים נגד הסתדרות המורים), לפיה על ההסתדרות להעביר את פרטי ההתקשרות אשר נמצאים במאגר לידי הסיעות המתמודדות בבחירות הפנימיות של הארגון (להלן "**החלטת בית הדין**").

3.7. על החלטת בית הדין הוגשה בקשה לביטול ההחלטה לבית המשפט המחוזי בתל-אביב, אשר דחה אותה ובהמשך לכך הוגשה בקשת רשות ערעור לבית המשפט העליון (רע"א 3351-16 יוסי וסרמן מזכ"ל הסתדרות המורים נ' גילה קליין) (להלן "**פסק הדין**"), אשר נדחתה. במסגרת החלטת בית המשפט העליון נקבע כי הסיעות בהסתדרות מהוות חלק מהארגון ועל כן יש לראות בהן כבעלות מאגר המידע ולאפשר להן לקבל גישה למאגר זה בעת תקופת הבחירות. יובהר כי לאחר כניסתו לתוקף של תיקון 13 בחודש אוגוסט 2025, שונה המונח "בעל מאגר", ל"בעל השליטה במאגר".

3.8. כמו כן, מאז ההחלטה בבית המשפט העליון התקבלו תקנות האבטחה (בחודש מרץ 2017), אשר נכנסו לתוקף בחודש מאי 2018. ההסתדרות פעלה ביחס לתקנות והתאימה פעולתה לציות מלא שלהן, מינתה ממונה אבטחת מידע תוך שהארגון שומר על שגרת אבטחת מידע בהתאם לדרוש בתקנות האבטחה ואף מעבר לכך.

3.9. במקביל למתואר לעיל ולאחר הליך פיקוח שנמשך מספר חודשים, ביום 28 ביוני 2018 מצאה הרשות להגנת הפרטיות כי הסתדרות המורים הפרה, לצד גורמים המזוהים עם סיעת ארגון מורי ישראל (אמ"י), הוראות הקבועות בחוק אשר בגינן הוחלט להטיל על ההסתדרות קנס מנהלי בגובה 25 אלף ש"ח וכן נדרשה ההסתדרות לערוך מספר תיקונים בשל ליקוי אבטחת מידע. ההסתדרות פעלה בהתאם לדרישה זו וכיום עומדת בדרישות אבטחת המידע הקבועות בחוק וכן בהוראות הרשות.

3.10. העובדות המתוארות לעיל עומדות, כפי שנפרט להלן, בבסיס מסקנותינו.

4. <u>דיון ומסקנות</u>

4.1. עינינו הרואות כי מאז החלטת בית המשפט העליון, הנזכרת לעיל, התרחשו ארבעה אירועים עובדתיים: נכנסו לתוקף תקנות אבטחת המידע, ניתנה החלטת הרשות להגנת הפרטיות במסגרת הפיקוח בהסתדרות, נכנס לתוקפו תיקון 13 לחוק הגנת הפרטיות ועודכן המאגר, כאשר כיום הוא אינו נדרש ברישום, אלא בהסדרה עצמית בלבד ובחובת ידוע לרשות להגנת

הפרטיות. בעניינו, כפי שנקבע בהחלטת בית הדין ומאוחר יותר בפסק הדין, הסיעות המתמודדות בהליך הבחירות בהסתדרות נחשבות כחלק מההסתדרות ולכן ניתן לראות בהן כחלק מבעלות המאגר. מובהר כי במסגרת תיקון 13 לחוק, תוקנו מספר הגדרות הקבועות בחוק, וביניהן גם הגדרת המונח "בעל מאגר מידע". חידוש מרכזי בהקשר זה הוא הוספת הגדרת המונח "בעל שליטה במאגר", אשר, בדומה למונח "Controller" ב-GDPR (General Data Protection Regulation של האיחוד האירופי), הוגדר בתיקון 13 כ"מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע, או ארגון שהוא, או בעל תפקיד מטעמו, הוסמך בחיקוק לעבד מידע במאגר מידע".

4.2. הלכה למעשה, תיקון 13 לחוק הביא להחלפת הגדרת "בעל מאגר מידע" בהגדרת "בעל שליטה במאגר מידע". משכך, יש לראות בסיעות המשתתפות בבחירות כ"בעלות שליטה" במאגר, בהתאם למשמעות המונח לאחר תיקון 13. ואולם, הן בהחלטת בית הדין והן בפסק הדין נקבע כי המידע שהותר להעברה לסיעות מוגבל לנתוני המאגר שאינם עונים להגדרה "מידע" ו"מידע רגיש" בחוק. יודגש, כי בעקבות תיקון 13 שונו אף הגדרות אלה, והן מוגדרות עתה "מידע אישי" ו"מידע בעל רגישות מיוחדת", בהתאמה.

4.3. מן האמור עולה, כי על אף שהסיעות הוכרו כבעלות שליטה במאגר, אין הן מוסמכות לקבל גישה מלאה או לעבד את כלל המידע המצוי בו, אלא נהנות מהרשאות גישה חלקיות בלבד, בהתאם למגבלות שנקבעו בפסק הדין. כפועל יוצא מכך, היקף החובות המוטלות עליהן מצומצם ואינו זהה להיקף החובות המוטלות על ההסתדרות, כבעלת השליטה הרחבה במאגר, לרבות חובות כגון מינוי ממונה על הגנת הפרטיות, ביצוע עדכון שנתי של המאגרים וכיוצא בזה.

4.4. קביעה זו, מקנה לסיעות זכות אך לצידן, למעשה, גם מחילה על הסיעות חובות מסוימות מכוח החוק והתקנות בכל הקשור להגנת המידע המצוי במאגר וכן לאופן השימוש בו. כלומר, לאחר שתעביר ההסתדרות את המאגר לידי הסיעות, יוכלו הסיעות לעשות שימוש במידע המצוי במאגר בהתאם לקבוע בחוק הגנת הפרטיות (ובכפוף להגבלות שהוצגו בהחלטת בית הדין ובפסק דין), קרי לפי עקרון צמידות המטרה וכל שימוש שלא לפי מטרות המאגר יהווה שימוש אסור אשר מנוגד לקבוע בחוק ואף במקרים מסוימים יכול לעלות לכדי אחריות פלילית ומנהלית.

4.5. כמו כן, על הסיעות להימנע מכל שימוש שלא ניתנה לגביו הסכמה של מושא המידע או שימוש החורג מההסבר, שניתן לו בדבר מטרת השימוש כפי שעולה מהנוסח המצורף.

4.6. בנוסף, בתור חלק מבעלות השליטה המאגר, על הסיעות יחולו החובות בנוגע לאבטחת המידע אשר מצוי במאגר, בהתאם להוראות החוק ותקנות אבטחת המידע. כך, שעל הסיעות, בין היתר, תוטל החובה להבטיח כי לא תהיה פגיעה במאגר, המידע שבמאגר יוחזק בדרכים מתאימות, לא יועבר לגורמים שאינם מורשים, ובדרכים שאינן מבטיחות את השימוש בו, ניהול הגישה למאגר, והכל לפי תקנות אבטחת מידע. בפסקה 10 לפסק הדין חידד בית המשפט העליון את סוגיית אבטחת המידע אשר קיבלו תוקף בתקנות האבטחה ויש לנקוט הצעדים הדרושים לשמירה על אבטחת המידע בדרך העולה בקנה אחד עם הוראות אלו. בהתאם לכך, אנו סבורים כי יש ליתן לממונה על אבטחת המידע בהסתדרות סמכויות פיקוח ואכיפה (להלן "**סמכויות הפיקוח**"), לצד העברת הרשימות מהמאגר לסיעות בארגון, על מנת להבטיח כי הסיעות אכן עומדות בדרישות החוק והתקנות.

4.7. לאור העובדה כי המאגר הוא מאגר מידע המצריך את רמת האבטחה הגבוהה, נדרש בעל השליטה במאגר לעמוד בדרישות המחמירות בחוק ובתקנות אבטחת המידע, כדוגמת קביעת נהלי אבטחה ארגוניים, ניהול הרשאות גישה, ביצוע סקר סיכונים אחת ל-18 חודשים ועוד. קיומן של חובות אלו מאפשרות לבעל השליטה במאגר להחזיק במאגר ולכן יש לקיימן מהרגע ההחזקה הראשון, כפי שמופרט בנוהל העברת המידע להן. כאמור לעיל, וכחלק מסמכויות הפיקוח תוטל על ממונה אבטחת המידע סמכות לבחון את קיומן של החובות האמורות וכן את התשתית להעברת המידע.

4.8. <u>קיום דרישות חוק הגנת הפרטיות בנושא דיוור ישיר</u>. לאור האמור במטרות המאגר, לאחר העברת המידע, יחולו על הסיעות החובות בחוק, ובתוך כך אף ביחס לנושא הדיוור ישיר, כפי שפרטנו לעיל בחלק המשפטי של מסמך זה. כך שבמידה שיחפצו לפנות בדיוור ישיר למושאי המידע, יעשו זאת תוך ציון כי הפנייה נעשתה בדיוור ישיר, זהות השולח, והמקורות מהם קיבל את המידע (הארגון) וכן את זכותו של הנמען להימחק מרשימת הדיוור במאגר.

4.9. <u>שימוש במידע מפנקס הבוחרים</u>. כאמור לפי חוקת ההסתדרות, עובר למועד הבחירות מופץ פנקס הבוחרים המכיל מידע אישי על הבוחרים וזאת בדומה למנגנון החל בבחירות לכנסת או לרשויות המקומיות. פנקס מידע זה הוא למעשה חלק ממאגר המידע של עובדי ההוראה המתואר לעיל, ולכן חלות עליו הוראות פרק ב' לחוק[5]. כאמור, בשל הדמיון הרב של מנגנון זה למנגנון הנהוג בבחירות לכנסת ולרשויות המקומיות, ניתן ללמוד כי גם בבחירות למוסדות ההסתדרות השימוש במידע שבפנקס יהיה בהתאם לצרכי התמודדות בבחירות ולצורכי קשר עם ציבור הבוחרים בתקופת הבחירות וכי אין לעשות בו שום שימוש אחר לרבות העברתו לאחר.[6] כמו כן, לאחר הבחירות על הסיעות לבער את עותקי המידע שמקורם בפנקס הבוחרים ולוודא כי אין הן מחזיקות במידע שמקורו בפנקס זה.

4.10. בנוסף, השימוש במאגר בתקופת הבחירות עולה לכדי שימוש לצורכי ההסתדרות ולכן, כאשר צורך זה לא יעמוד בתוקפו, קרי, לאחר מועד הבחירות ובחירת המוסדות, על הסיעות יהיה להשמיד את המאגר המצוי ברשותן ולוודא כי אינן עושות שימוש בו בתקופה שאחריה.

4.11. לאור האמור לעיל, על מנת שההסתדרות תוכל להבטיח כי תעמוד בכל הוראות החוק המחייבות אותה בתור בעלת המאגר, העברת המידע לסיעות השונות תבוצע בכפוף לנוהל העברת מידע סדור (אשר נוסחו מופיע כ**נספח ב'** לחוות דעת זו) (להלן "**נוהל העברת המידע**").

4.12. נוהל העברת המידע יהיה נוהל מחייב לצורך העברת מידע לסיעות לקראת הבחירות למוסדות ההסתדרות והחותמים עליו יקבלו על עצמם את האחריות בגין העברת המידע והחזקתם במידע.

4.13. בנוסף, יתחייבו הסיעות, כחלק מנוהל העברת המידע, כי לאחר הבחירות ימחקו הסיעות השונות את המידע שהתקבל כחלק מהעברת המידע.

5. <u>אחרית דבר</u>

[5] הרשות להגנת הפרטיות, מגבלות השימוש במידע מפנקס הבוחרים ומגבלות השימוש במידע אישי – ריענון הוראות חוק הגנת הפרטיות לקראת הבחירות לרשויות המקומיות לשנת 2018. עמ' 2.

[6] סעיף 39(ג) לחוק הבחירות לכנסת [נוסח משולב], תשכ"ט-1969 וכן סעיף 16 לחוק הרשויות המקומיות (בחירות), תשכ"ה-1965.

5.1 מסמך זה מחווה דעה לגבי סוגית העברת המידע ממאגר המידע של ההסתדרות, לסיעות המתמודדות לבחירות במוסדות ההסתדרות. מסמך זה מציע, מפרט ומבהיר את אופן הפעולות בהם על ההסתדרות והסיעות לפעול ואת חובותיהן, הן במסגרת בהתאם לחוק הגנת הפרטיות, תקנות האבטחה וההנחיות השונות. לאור ההליכים שבוצעו בהסתדרות בהיבט דיני הפרטיות בשנים האחרונות, שכללו בין היתר את הליך הפיקוח מטעם הרשות להגנת הפרטיות ואת תגובת ההסתדרות, וכן את ההסדרה שביצעה הרשות לקראת כניסתו לתוקף של תיקון 13 לחוק, וזאת על מנת לעמוד בתקנות השונות ובחוק אנו בדעה כי העמידה באמור במסמך זה תשרת את טובת הצדדים ותבטיח כי העברת המידע תבוצע בהתאם להוראות החוק השונות.

5.2 מדובר בנושא מורכב המגולל בתוכו באופן אינהרנטי היבטים הנוגעים לזכות לפרטיות בעולם טכנולוגי אשר לעולם אינו שוקט על השמרים. בשל כך, הוקדשה במסמך זה תשומת לב מיוחדת לשילוב בין העולם המשפטי / מסחרי לבין העולם הטכנולוגי היישומי, שכן יש ביניהם קשר הדוק ליכולתה של ההסתדרות לנהל את פעילותה במערכת הבחירות בהתאם להוראות הדין בכלל ובדיני הפרטיות בפרט.

5.3 המסקנות נשוא חוות דעת זו מבוססות על הממצאים העובדתיים כפי שנמסרו לנו על-ידכם. ככל שהממצאים המתוארים במסמך זה אינם נכונים ו/או מדויקים, ייתכן כי מסקנותינו ישתנו בהתאם.

5.4 נשמח לעמוד לרשותכם בכל שאלה ו/או הבהרה, ככל שתידרשנה בעניין זה ובכלל.

_____	_____
ד"ר דן חי, עו"ד	תומר פינקלשטיין, עו"ד

דן חי ושות', משרד עורכי-דין

נספח א' – נוסח הסכמה

בעת הצטרפות חבר חדש לשורות ההסתדרות, יאשר הלקוח הסכמתו בחתימה להודעה על פי הדוגמא הבאה:

"הנני נותן הסכמתי כי הפרטים שמסרתי לעיל יחייבו אותי בכל עניין הנוגע לחברותי בהסתדרות המורים וישמשו לדיוור ישיר באמצעים שונים ובכללם פקסימיליה, מערכת חיוג אוטומטית הודעה אלקטרונית, הודעת מסרון וכיוב' בהתאם לצורכי הסתדרות המורים, לרבות לצורך שיווק שירותים, מוצרים, הטבות והנחות המיועדות לחברי הסתדרות המורים.

ידוע לי, כי בכל שלב אוכל להודיע בכתב להסתדרות המורים על רצוני להפסיק קבלת דבר הפרסומת.

טופס זה ייסרק ויירשם במאגר הסתדרות המורים וישמש לטיפול מקצועי ולצורכי דיוור ישיר לחברים."

נספח ב'

בחירות למוסדות הסתדרות המורים בישראל – פברואר 2026

נוהל העברת מידע

ביום 17 בפברואר 2026, יתקיימו בחירות (להלן "**הבחירות**") במוסדות הסתדרות המורים בישראל (להלן "**ההסתדרות**"). כחלק מהליך הבחירות מעבירה ההסתדרות לסיעות השונות מידע המצוי במאגר המידע שבשליטת ההסתדרות (מאגר מידע "עובדי הוראה") (להלן "**מאגר המידע**") וכן מידע מספר הבוחרים (להלן "**העברת המידע**"). נוהל העברת מידע זה נועד להבטיח כי העברת המידע תהיה בכפוף להוראות חוק הגנת הפרטיות, התשמ"א- 1981 (להלן "**החוק**"), הנחיות הרשות להגנת הפרטיות, תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן "**תקנות אבטחת המידע**") וכל הוראת חוק רלבנטית אחרת.

נוהל העברת המידע יחייב כל סיעה המתמודדת בבחירות (להלן "**הסיעה**"), המעוניינת לקבל את המידע, כלפי ההסתדרות וחבריה אשר המידע אודותם מצוי במאגר המידע.

נוהל העברת מידע זה נועד להבטיח, כי כל ראש סיעה אשר תבקש לקבל מידע ממאגר המידע ומספר הבוחרים, בבחירות למוסדות ההסתדרות שיערכו ביום 17 בפברואר 2026, יתחייב בחתימתו כי הוא והסיעה יפעלו כדלהלן:

(1) לפעול בכפוף להוראות כל דין, לרבות, אך לא רק, חוק הגנת הפרטיות ותקנותיו ובמיוחד תקנות אבטחת המידע, ולרבות שימוש במידע שבמאגר אך ורק למטרה הרשומה של המאגר ולצורך הבחירות.

(2) לקיים אחר חובת סודיות במידע שבמאגר ובתוך כך, לשמור בסודיות מוחלטת ולא להעביר או לגלות, בין במישרין ובין בעקיפין, לצד שלישי כלשהו (בארץ ובחו"ל), בין בתמורה ובין שלא בתמורה, את המידע כאמור, ללא הסכמתה של ההסתדרות מראש ובכתב ולדאוג לאסור על כל אדם מטעמו, הבא במגע עם המידע שבמאגר מתוקף תפקידו, לגלות את אותו מידע אלא לצורך ביצוע עבודתו או לביצועו של החוק. התחייבות זו של המועמד תהא ללא הגבלת זמן.

(3) לפעול כך שנתונים ומידע אשר יועברו אליו מהסתדרות, יאובטחו בהתאם להוראות תקנות האבטחת המידע כך שלא תתאפשר גישה, בין באופן אקטיבי ובין באופן פאסיבי, למידע ולנתונים אלו, לאיש מלבד המורשים לכך מטעמו. למען הסר ספק מובהר, כי התחייבות זו מתייחסת הן למערכות, מאגרים, סיסמאות, הרשאות, המחשבים והשרתים שיהיו ברשות המועמד והסיעה, והן לאבטחה הפיזית של המידע, כגון נעילתו, שמירתו, קיום נהלי טיפול ברורים וכיו"ב.

(4) לקבוע אחראי בכל סיעה לנושא אבטחת מידע וכן להגדיר את מורשי הגישה הבלעדיים למאגר ולדאוג להחתים אותם על התחייבות למלא נוהל זה. רשימת המורשים תועבר להסתדרות קודם להעברת החומר למועמד. הרשימה תוחזק על-ידי אחראי אבטחת המידע שיקבע ותוצג בכל מקרה של ביקורת של ההסתדרות או הרשויות המוסמכות.

חל איסור לבצע כל שינוי, הוספה או גריעה ברשימת מורשי הגישה שצויינה לעיל ללא קבלת הסכמה מפורשת ובכתב מממונה אבטחת המידע בהסתדרות.

(5) לעמוד בכל דרישות הוראות חוק הגנת הפרטיות ותקנות האבטחה בכל הקשור לחובות המוטלות על מאגרי מידע ברמת האבטחה הגבוהה. כך בין היתר ביצוע סקר סיכונים ובחינת עמידות המערכת בפני ניסיונות חדירה ; עמידה בתקני האבטחה הדרושים ועוד. הממונה על אבטחת המידע בהסתדרות יבדוק ויאשר את העמידה בתקנות לפני קבלת המידע וזאת לפי הסטנדרטים הנהוגים בהסתדרות כיום.

(6) לאפשר לממונה אבטחת המידע בהסתדרות להפעיל את סמכויות הפיקוח הנתונות לו לשם בחינה ופיקוח אחר קיום דרישות הוראות חוק הגנת הפרטיות ותקנות האבטחה.

(7) סיעה המבקשת למנות ממונה לאבטחת מידע משלה רשאית לעשות כן ובלבד שזהות ממונה אבטחת המידע שתבחר תאושר על ידי הממונה על אבטחת המידע של ההסתדרות וכך יאושרו מראש הליכי הבדיקה ותוצאותיה שיבצע אותו ממונה.

(8) לדאוג כי עיבוד המידע שיימסר לו יתבצע בהתאם למטרות הברורות והלגיטימיות של ההסתדרות ומטרת המאגר כפי שמופיעות כיום. בכל מקרה של ספק אם הפעולה המבוקשת עולה בקנה אחד עם מטרת המאגר, יש לפנות ולהיוועץ עם ממונה אבטחת המידע בהסתדרות.

(9) להתחייב כי המידע אשר הועבר אליו על-ידי ההסתדרות ישמש אך ורק לצורך פעולות פוליטיות הקשורות באופן ישיר לבחירות, ובהתאם למטרות המוגדרות לכך ולא מעבר לכך.

(10) למלא באופן מידי אחר בקשות הסרה מרשימת הדיוור של מאגר המידע, על-ידי מושאי המידע שבמאגר, בין שיגיעו במישרין ובין פניות שיגיעו דרך ההסתדרות ולעדכן את ההסתדרות על כל בקשה כזו אחת ליום.

(11) להודיע להסתדרות מיד לכשייוודע לו על כל נזק שנגרם לנכסי המידע של ההסתדרות, לרבות כל חשיפה, דליפה, שינוי או מחיקה של מידע.

(12) להמציא להסתדרות, בתוך 7 ימים מיום הבחירות, תצהיר מאומת כדין על ידי עו״ד, על-פיו המידע שהועבר לידיו במהלך תקופת הבחירות וכל עותקיו והמידע המצוי בו נמחקו והושמדו וכן כי לא נותרו בידי ו/או בידיו של צד ג׳ כלשהו ולא ניתן לשחזר אותם. ככל והמועמד ייטול חלק בסיבוב השני של הבחירות, ככל ויהיו, יחול האמור ביחס למועד הבחירות בסיבוב השני.

אישור הסיעה

הנני מצהיר ומאשר כי קראתי את נוהל העברת המידע של ההסתדרות הנ"ל ומתחייב לפעול על-פיו, כי אהיה אחראי כלפי ההסתדרות באחריות כוללת גם על מעשי ו/או מחדלי ו/או רשלנות כל מי מטעמי ו/או כל ספק משנה מטעמי, ככל שיהיו.

לראיה באתי על החתום:

שם המועמד: _____

שם הסיעה: _____

תאריך: _____

חתימה: _____

<u>מתן ערבות מטעם הסיעה</u>:

סיעה אשר תבקש לקבל את המידע כאמור לעיל תידרש לחתום על טופס ערבות שתמומש ככל הצורך בתוך 7 ימים מיום הבחירות במידה ולא יימסר להסתדרות תצהיר מאומת על-פיו המאגר וכל עותקיו הושמדו.

<u>ערבות</u>

אני הח"מ: _____, ת.ז. _____, העומד בראש סיעת _____ ערב בשם הסיעה, בערבות בלתי מותנית ובלתי חוזרת כלפי הסתדרות המורים בישראל (להלן- "**ההסתדרות**"), לכל נזק שיגרם להסתדרות אם ידלוף מידע בניגוד לנוהל העברת מידע. כמו כן, להמציא להסתדרות בתוך 7 ימים מיום הבחירות תצהיר מאומת כדין על ידי עו"ד, על פיו מאגר המידע וכל עותקיו נמחקו והושמדו ולא ניתן לשחזר אותם. ידוע לי כי ככל ויתברר להסתדרות כי לא קיימתי את האמור לעיל, יהיה עלי לשאת מיד עם דרישת ההסתדרות בתשלום בסך 20,000 ₪ לזכות ההסתדרות וזאת ללא כל הוכחת עילה או נזק מצד ההסתדרות. למען הסר ספק אני מצהיר ומאשר כי אין בסכום הנ"ל בכדי לגרוע בכל עילה ו/או טענה ו/או סעד אחר לו זכאית ההסתדרות ע"פ כל דין ואין בו כדי לפטור מהחובה למחוק ולהשמיד את כל עותקיו של מאגר המידע ולהעביר תצהיר מאומת כדין על כך לידי ההסתדרות.

אני מצהיר כי הנני מקבל על עצמי ערבות זו לאחר שהבנתי את מהות התחייבותי שבכתב ערבות זה.

ולראיה באנו על החתום:

שם המועמד: _____

שם הסיעה: _____

תאריך: _____

חתימה: _____