<u>לרגל חודש הקניות – המלצות ללקוחותינו לאור ריבוי אירועי אבטחה באתרי האינטרנט</u>

לקוחות יקרים,

בעת האחרונה ליווינו מספר לקוחות, אשר אתרי האינטרנט אותם הם מפעילים, נחשפו לאירועי אבטחת מידע. המדובר בלקוחות, שפרטים רגישים, אודות משתמשים מתוך האתר שלהם, דלפו ו/או פורסמו באופן נגיש ברשת, או שבאתריהם זוהו פרצות אבטחה.

כידוע, כל ארגון ובפרט כזה הפועל ברשת האינטרנט, חשוף למתקפות סייבר ואירועי אבטחת מידע, כדוגמת האירועים לעיל וכדוגמת אלו עליהם אנו שומעים בתקשורת חדשות לבקרים. על הארגון לדעת כי בקרות אירוע אבטחה, מלבד החשיפה לאחריות פלילית ו/או נזיקית לארגון ו/או לבעלי תפקידים בו, האמור מחייב דיווח לרשות להגנת הפרטיות (להלן: "**הרשות**"), והיא מוסמכת, בין היתר, להורות לארגון לפרסם פרטים אודות האירוע ואף להודיע עליו באופן אישי ללקוחות הארגון, שפרטיהם דלפו (או שיש חשש לגבי דליפתם). **לפיכך, אירוע אבטחה עלול לגרום גם לפגיעה במוניטין ובאמון הלקוחות של הארגון וכתוצאה מכך לנזקים כלכליים, ולנזקים נוספים הנובעים מכך**. מעבר לסמכות הרשות בקשר עם אירועי אבטחה, לרשות סמכויות נרחבות בתחומי הפיקוח, החקירה, האכיפה והענישה. סמכויות, אותן הרשות מממשת ביתר שאת בשנים האחרונות בקרב מגזרים רבים במשק הישראלי הן במסגרת פיקוח רוחב אקראיים והן עקב אירועי אבטחה כאמור.

לרגל חודש נובמבר, הידוע כחודש הקניות העולמי, ריכזנו עבורכם רשימת המלצות בתחום הגנת הפרטיות, אשר עשויות לצמצם את החשיפות שתוארו לעיל. את ההמלצות להלן מוצע ליישם בקשר עם הפעלת אתרים, אפליקציות ואמצעים דיגיטליים נוספים (להלן: "אתר/ים"), במסגרתם נאסף מידע אודות לקוחותיכם ו/או אשר באמצעותם ניתן לבצע רכישות.

1. **אבטחת מידע באתר ובארגון** – ודאו כי אתרכם מאובטח ומוגן מפני פריצות ותקיפות ע"י גורמים עוינים וכי נעשה שימוש באמצעי אבטחה מתקדמים. ודאו כי מאגרי המידע בהם מעובד מידע המגיע מהאתר, מאובטחים ומוסדרים בהתאם לדרישות חוק הגנת הפרטיות, התשמ"א – 1981, התקנות מכוחו ודרישות הרשות להגנת הפרטיות (להלן: "**דיני הגנת הפרטיות**") ובין היתר, כי הנכם מחזיקים במסמכים הנדרשים לצורך עמידה בהוראות דיני הגנת הפרטיות (למשל: מסמך הגדרות מאגר, נוהל אבטחת מידע, מסמך מיפוי מאגר ועוד).
2. **יידוע, שקיפות ובהירות** – ודאו כי באתרכם מוטמעים מסמכים משפטיים, כגון: מדיניות פרטיות, תנאי שימוש ומדיניות קוקיז (ככל שנעשה שימוש בכלי זה). ודאו כי המסמכים הנ"ל עדכניים, כתובים בשפה פשוטה ובהירה ומספקים מידע מפורט ביחס לנעשה עם המידע שנאסף, לזכויות לקוחותיכם (אודותם נאסף המידע), לגורמים אליהם מועבר המידע והסיבות להעברה ועוד.
3. **מינימליזם** – ודאו כי אתם אוספים רק את הנתונים הדרושים לכם לצורך מתן השירותים המוצעים באתר וכי לא נאסף מידע "עודף".
4. **מודעות לפרטיות** – ודאו כי עובדי הארגון מודעים לחשיבות ההגנה על הפרטיות לקוחותיכם , בין היתר, באמצעות ביצוע הדרכות שוטפות, פרסום ואכיפת נהלי אבטחה.

5. **העברה לצדדים שלישיים** – ודאו כי ספקי שירותי אחסון הענן/ ניהול אתר/ סליקה וכן גורמים נוספים המקבלים גישה למידע שנאסף מלקוחותיכם– מאבטחים ושומרים על המידע כראוי ועושים שימוש במידע רק לצורך המטרה שלשמה נמסר המידע מלכתחילה. העברת מידע לצד שלישי, טומנת בחובה סיכונים לפרטיות לקוחותיכם. לפיכך, באחריותכם להסדיר במסגרת הסכם מפורט עם הצד השלישי, את מטרות העברת המידע, השימוש שרשאי לעשות, משך הזמן שבמסגרתו יהא רשאי להשתמש ולשמור את המידע, אמצעי אבטחת המידע שעליו לנקוט בקשר עם המידע ועוד.

לסיכום, הסדרת היבטי הפרטיות בארגון ובאתרים שהוא מפעיל הכרחית לצורך הגנה ושמירה הן על הארגון והן על לקוחותיו.
לצד זאת, יש לזכור כי ארגון המוכר מוצרים ושירותים לקהל הרחב, נדרש להסדיר פעילותו בתחומים נוספים כגון צרכנות, נגישות ועוד. משרדנו מעניק ייעוץ משפטי גם בנושאים אלו ומספק פתרונות הוליסטיים ללקוחותיו.

נשמח לעמוד לרשותכם בכל שאלה,

עו"ד גפנית לגזיאל שבבו, שותפה במחלקה המסחרית וראש תחום הגנת הפרטיות

עו"ד אורן שטריט טובה

***מובהר כי האמור במסמך זה הינו סקירה כללית ואין בו כדי להוות חוות דעת משפטית ו/או תחליף לקבלת ייעוץ משפטי פרטני.**