מדיניות הרשות להגנת הפרטיות בנוגע לקבלת דיווח אירוע אבטחה חמור

ביום 8.5.2018 ייכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017 (להלן - **התקנות**). לקראת מועד זה, מפרסמת הרשות להגנת הפרטיות (להלן - **הרשות**) מסמך המציג את עיקרי מדיניות הרשות לגבי דיווחי אבטחה מכח התקנות.

מדיניות זו נכונה למועד פרסומה, והרשות רשאית לעדכנה ולשנותה מעת לעת בהתאם לצורך ולשינוי הנסיבות. מומלץ לעקוב אחר העדכונים באתר.

1. מטרת המדיניות

1.1. במסגרת הערכות הרשות להטמעת התקנות ערכה הרשות שיחות עם מומחי אבטחת מידע וגורמים שונים במשק. שיחות אלה העלו כי הדיווח על אירוע אבטחה חמור הנדרש מכח התקנות (להלן - **אירוע**), עשוי להיתפס כמאיים בקרב בעלי המאגרים הכפופים לחובה זו, החוששים כי דיווח לרשות עשוי לחשוף אותם לתביעות ופעולות אכיפה מצד הרשות.

1.2. מדיניות סדורה המתייחסת לאופן הטיפול בדיווחים ולשיקול הדעת באכיפה, תסייע בהטמעת חובת הדיווח במשק, הגברת הוודאות באשר למקרים המחייבים דיווח לצד מקרים שאינם מחייבים דיווח.

1.3. בנוסף, במסגרת מדיניות זו הוחלט על תקופת מעבר ליישום התקנות (כמפורט בטבלה בהמשך מסמך זה) הכוללת הקלות כלפי המדווחים, לצד הפעלת סנקציות כלפי מפרי חובת דיווח.

2. אופן הטיפול בדיווח על אירוע אבטחה חמור

2.1. תקנה 11 לתקנות קובעת כי בעל מאגר מידע שחלה עליו חובת אבטחה בינונית או גבוהה (כהגדרתן בתקנות) מחויב להודיע באופן מיידי לרשות על אירוע אבטחה חמור וכן ידווח לרשות על הצעדים שנקט בעקבות האירוע.

2.2. ככלל, על הדיווח להתבצע תוך 24 שעות ממועד גילויו של האירוע ובכל מקרה לא יאוחר מ-72 שעות מאותו מועד.

2.3. חובת הדיווח חלה על בעל המאגר, מנהל המאגר ומחזיק המאגר, בנפרד אולם די בדיווח יחיד על אירוע כדי לקיים את החובה עבור שלושת הגורמים גם יחד.

2.4. דיווח על אירוע אבטחה חמור יתבצע באמצעות טופס דיווח מקוון (להלן - **טופס הדיווח הראשוני**) המפורסם באתר האינטרנט של הרשות [טופס הדיווח].

2.5. אופן מילוי טופס הדיווח הראשוני, לרבות דוגמאות לאירועים המחייבים דיווח לעומת אירועים אשר בשלב זה הרשות אינה מתכוונת לאכוף את חובת הדיווח עליהם - אף אם הם עשויים להיחשב כאירועי אבטחה חמורים - מופיעים באתר הרשות.

2.6. הרשות תבחן את פרטי הדיווח, ונציג הרשות ייצור קשר עם הגורם המדווח על מנת לאמת את המידע ובמידת הצורך לקבל פרטים נוספים אודות האירוע, ובכדי לקבוע האם יש צורך בפרטים נוספים (במילויו של טופס דיווח מורחב שיועבר למדווח בכדי לאסוף פרטים נוספים הנדרשים לשם בחינת אופן הטיפול באירוע).

2.7. לאחר קבלת כל הפרטים הנדרשים לגבי האירוע, תקבע הרשות את חומרת האירוע, בין היתר בהתחשב בקריטריונים הבאים: רגישות המידע שדלף, מקור הנזק, היקף דלף המידע, האם המידע דלף בפועל מחוץ לארגון או שרק קיים סיכון שידלוף, כמות נושאי המידע שיש חשש שמידע אודותיהם דלף, הנזק שעלול להיגרם לנושאי המידע, הנזק שעלול להיגרם לגורם המדווח, למגזר או למשק, והתנהלות הארגון בקשר עם האירוע ומוכנותו.

2.8. בהתאם לסיווג חומרת האירוע, תקבע הרשות את המשך הטיפול באירוע - קביעת הנחייה להמשך מעקב אחר הטיפול באירוע, קביעת הנחיות לתיקון ליקויים, פיקוח או חקירה בחצרי הגורם המפוקח, קביעה פורמלית כי הגורם המפוקח הפר את הוראות החוק ו/או התקנות, ובמקרים המתאימים הטלת סנקציות לרבות התלייה או ביטול רישום המאגר, בכפוף למתן זכות שימוע. בנוסף, תקבע הרשות האם נדרש להודיע על האירוע לנושאי המידע שעלולים להיפגע מן האירוע, ועל אופן ההודעה ותזמונה.

2.9. בהחלטה להודיע על אירוע אבטחה חמור לנושאי המידע יילקח בחשבון האם המידע האישי אכן דלף בפועל או שרק קיים סיכון לכך שידלוף, וכן מה מידת הנזק הצפויה לנושאי המידע. ההחלטה לחייב הודעה לנושאי המידע תבוצע בהתייעצות עם מערך הסייבר, ובהתאם לנסיבות גם בתיאום עם הרגולטור המגזרי.

2.10. קביעת הפרה כמתואר לעיל, תפורסם באתר הרשות ו/או באופן פומבי אחר, על פי שיקול דעתה של הרשות.

2.11. במקרה שהרשות הנחתה לבצע תיקון ליקויים בעקבות האירוע, ינוהל מהלך בקרה בו יעדכן הגורם המפוקח את הרשות באשר לתהליך תיקון הליקויים, והרשות תהיה רשאית לערוך בקרה בנושא.

2.12. יודגש כי אי דיווח כנדרש על פי התקנות או הפרת הוראות הרשות מהוות הפרה בפני עצמה, ולרשות עומדות סמכויות האכיפה כמפורט בחוק.

3. יישום הסמכות - אכיפה הדרגתית

לאור ההערכות הנדרשת מבעלי, מנהלי ומחזיקי מאגרי מידע, החליטה הרשות לנקוט במדיניות אכיפה סובלנית כלפי המדווחים על אירוע אבטחה חמור בתקופת ההטמעה הראשונית ותקופת הביניים כמפורט להלן:

	לוח זמנים	אכיפה בעקבות דיווח	אכיפה במקרה של ממצאים חריגים	אכיפה במקרה של אי דיווח
תקופת הטמעה ראשונית	**עד 31 בדצמבר 2018**	הנחייה לתיקון ליקויים	קביעת הפרה, במידת האפשר תוך הימנעות מפרסום	קביעת הפרה ופרסומה (כולל פרסום אי הדיווח), התלייה או ביטול רישום המאגר
תקופת הביניים	**עד 30 ביוני 2019**	במקרים קלים – הנחייה לתיקון ליקויים, ביתר המקרים – קביעת הפרה	קביעת הפרה	קביעת הפרה ופרסומה (כולל פרסום אי הדיווח), התלייה או ביטול רישום המאגר
יישום מלא	**החל מה- 1 ביולי 2019 ואילך**	קביעת תוצר אכיפתי רגיל ע"פ מדיניות הרשות	קביעת תוצר אכיפתי רגיל ע"פ מדיניות הרשות	קביעת תוצר אכיפתי רגיל ע"פ מדיניות הרשות (כולל פרסום אי הדיווח), התלייה או ביטול רישום המאגר

מובהר כי כל המתואר לעיל מבטא מדיניות כללית בלבד, והרשות רשאית להקל או להחמיר במדיניות זו, בהתאם לנסיבות כל אירוע, מידת חומרתו, היקף הנזק והיקף נושאי המידע.