יולי 2018

GORNITZKY
80 Years of Excellence

חובת הדיווח על אירועי אבטחת מידע
*(data breach notification)

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: **"התקנות"**), שנכנסו לאחרונה לתוקף, מטילות חובות מקיפות בתחום אבטחת המידע על חברות שמחזיקות או שבבעלותן מאגרי מידע הכוללים מידע אישי (לרבות, מאגר מידע על עובדי החברה או לקוחותיה). תקנה 11(ד) לתקנות מחייבת את בעל מאגר המידע, המחזיק בו ומנהל המאגר לדווח באופן מיידי לרשם מאגרי המידע (להלן: **"הרשם"**) על כל אירוע אבטחה חמור הנוגע למידע המוחזק במאגר.
נעמוד להלן בתמצית על חובת הדיווח על אירועי אבטחה לפי התקנות ועל אופן יישומה.

1. ביחס לאילו סוגי מאגרי מידע עשויה לקום חובת הדיווח?

חובת הדיווח עשויה לקום ביחס לכל מאגר מידע שחלה עליו, לפי התקנות, "רמת האבטחה הבינונית" או "רמת האבטחה הגבוהה".

ככלל, רמת האבטחה הבינונית חלה על מאגרי מידע הכוללים מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מידע רפואי, מידע על עבר פלילי, מידע על אמונה דתית וכדומה ועל מאגרי מידע שמטרתם העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק. רמת האבטחה הגבוהה חלה ככלל על מאגר מידע המקיים את התנאים לתחולת רמת האבטחה הבינונית, אם במאגר המידע קיים מידע על 100,000 אנשים או יותר או אם מספר בעלי ההרשאה במאגר עולה על 100.

2. באילו מקרים קמה חובת הדיווח?

חובת הדיווח קמה ביחס ל-"אירוע אבטחה חמור". במאגר מידע שחלה עליו רמת האבטחה הגבוהה, הכוונה היא לכל אירוע בו נעשה שימוש במידע מן המאגר בלא הרשאה או בחריגה מהרשאה, או שנעשתה פגיעה בשלמות המידע. במאגר מידע עליו חלה רמת האבטחה הבינונית, חובת הדיווח קמה אם השימוש או הפגיעה כאמור נעשו ביחס לחלק מהותי מן המאגר.

הרשות להגנת הפרטיות (**"הרשות"**) פרסמה לאחרונה דוגמאות לאירועי אבטחה חמורים המחייבים דיווח לרשם. הדוגמאות, אשר מתייחסות למאגרי מידע שחלה עליהם רמת האבטחה הגבוהה, כוללות בין היתר, את האירועים הבאים:

א. זיהוי של פריצה (חיצונית או פנימית) לרשת הארגון, במסגרתה קיים חשש סביר או וודאות כי הפורץ ניגש למאגר מידע של הארגון.

ב. העברה של מידע אישי ממאגרי המידע של הארגון על ידי עובד הארגון אל מחוצה לו, ללא אישור או הרשאה.

ג. גניבה/אבדן של ציוד מחשוב, מדיה נתיקה או אמצעי פיזי לגיבוי המכילים מידע אישי מתוך מאגר המידע של הארגון, או העברתו לגורם חיצוני שאינו אמור להיות נגיש למידע.

ד. התפרצות של וירוס כופר אשר שיבש או הצפין מידע מתוך מאגר מידע של הארגון, ללא יכולת שחזור המידע.

3. תוך כמה זמן יש לדווח לרשם על אירוע אבטחה חמור?

תקנה 11(ד) מחייבת דיווח לרשם "באופן מיידי". עמדת הרשות, כפי שמוצאת ביטוי במסמך מדיניות שהרשות פרסמה לאחרונה בנושא ("**מסמך המדיניות**"), היא כי על הדיווח להתבצע ככלל בתוך 24 שעות ממועד גילוי האירוע ובכל מקרה לא יאוחר מ-72 שעות מאותו מועד.

4. כיצד מתבצע הדיווח לרשם?

הדיווח מתבצע באמצעות טופס דיווח מקוון באתר הרשות.

5. כיצד הרשות מתכוונת לטפל באירועים אשר דווחו כראוי?

במסמך המדיניות, הרשות ציינה כי תנקוט מדיניות אכיפה סובלנית כלפי המדווחים על אירועי אבטחה חמורים בתקופה שעד ליום 31.12.2018 (תקופת ההטמעה הראשונית) ובתקופה שעד ליום 30.6.2019 (תקופת הביניים). מסמך המדיניות כולל פרטים נוספים באשר למדיניות האכיפה בתקופות הנ"ל.

6. האם התקנות מחייבות דיווח גם לאדם שמידע עליו נחשף (נושא המידע) כתוצאה מאירוע האבטחה החמור?

התקנות אינן מחייבות את בעל המאגר, מנהל המאגר או המחזיק בו לדווח ישירות לנושא המידע על אירועי אבטחה. אולם, לפי סעיף 11(ד) לתקנות, הרשם רשאי, לאחר היוועצות עם ראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע. מסמך המדיניות מבהיר כי בהחלטה האם להודיע לנושא המידע, הרשם יבחן האם המידע האישי אכן דלף בפועל וישקול את חומרת הנזק הצפוי לנושא המידע.

7. כיצד ניתן להיערך לקיום חובת הדיווח לפי התקנות?

לפי התקנות, בעל מאגר המידע, המחזיק בו ומנהל מאגר המידע אחראים על תיעוד אירועי אבטחה, אף אם אין מדובר באירועים "חמורים". כמו כן, קיימת חובה להגדיר בנוהל אבטחת המידע של החברה הוראות לעניין התמודדות עם אירועי אבטחה, לפי חומרת האירוע ומידת רגישות המידע. במסגרת זו, מומלץ להסדיר אף את האופן בו החברה תקיים את חובת הדיווח לרשם, לרבות תוך הסדרת מנגנון לדיווח פנימי בתוך החברה על אירועי אבטחה. במקביל, יש להגביר את המודעות של עובדי החברה לחובות לפי התקנות, לרבות חובת הדיווח לרשם על אירועי אבטחה חמורים.

בנוסף לדרישת הדיווח לפי התקנות, חשוב שהחברה תיערך אף לקיום חובות הדיווח אשר עשויות לחול עליה מכוח הנחיות רגולטוריות (למשל, החובה שחלה על גופים מוסדיים לדווח על אירועי סייבר לממונה על שוק ההון, הביטוח והחיסכון) או מכוח דין זר (לדוגמא, חובת הדיווח לרשויות האירופאיות מכוח הרגולציה האירופאית בתחום הגנת המידע – GDPR).

לפרטים נוספים:

עו"ד אסף הראל, שותף

assafh@gornitzky.com

עדכון לקוחות זה נכתב בסיועו של מר תומר פרושאור

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנדונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.