מאי 2017

GORNITZKY&CO

תקנות חדשות מטילות חובות בתחום אבטחת המידע על קשת רחבה של עסקים הפועלים במשק*

בקרוב צפויות להתפרסם תקנות חדשות, המסמנות מהפכה של ממש בדרישות הרגולטוריות בתחום הסייבר ואבטחת המידע. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("התקנות"), שאושרו לאחרונה על-ידי ועדת חוקה חוק ומשפט של הכנסת, מטילות שורה של חובות מקיפות על מי שמחזיק**, מנהל או שבבעלותו מצוי מאגר מידע הכולל מידע אישי, בהתאם למאפייני המאגר. בשונה מהרגולציה עד כה בתחום הגנת הסייבר ואבטחת המידע, שהתמקדה במגזר הציבורי ובמגזרים מפוקחים (כגון בנקים וחברות הביטוח) התקנות החדשות מחייבות כל עסק (ובהיבטים מסוימים אף יחיד) המחזיק מידע אישי על עובדים, לקוחות או ספקים, בין אם מדובר בחברה ציבורית או בעסק בינוני או קטן, לעמוד בסטנדרטים החדשים.

היקף החובות שיוטלו על עסק מסוים אינו מושפע מגודלו או מהיקף הכנסותיו, אלא ממטרת מאגר המידע שברשותו (למשל, האם המידע נאסף לשם מתן שירותי דיוור ישיר), סוג המידע האגור במאגר (למשל, האם מדובר במידע ביומטרי, במידע על נכסיו של אדם או במידע על התנהגותו ברשות היחיד), מספר האנשים שמידע עליהם מוחזק במאגר ומספר מורשי הגישה אל המאגר. על בסיס פרמטרים אלה, התקנות מבחינות בין ארבעה סוגי מאגרים: מאגר המנוהל בידי יחיד, מאגר שחלה עליו רמת אבטחה בסיסית, מאגר שחלה עליו רמה אבטחה בינונית ומאגר שחלה עליו רמת אבטחה גבוהה.

להלן מספר דוגמאות לחובות שיוטלו מכוח התקנות החדשות:

- **נוהל אבטחת מידע-** התקנות מחייבות לגבש, ולבחון מחדש אחת לשנה לפחות, נוהל אבטחת מידע אשר יפרט, בין השאר, את הסיכונים שחשוף להם המידע שבמאגר, אופן הטיפול בסיכונים אלה, אופן ההתמודדות עם אירועים של שימוש בלתי מורשה במידע שבמאגר, מורשי הגישה למאגר ועוד. במסגרת זו, קיימת דרישה לבחון, אחת לשנה, האם המאגר אינו כולל מידע רב מן הנדרש למטרות המאגר.
- **מיפוי מערכות המאגר וסקר סיכונים** – יש לגבש ולהחזיק מסמך מעודכן של מבנה מאגר המידע ורשימת מצאי מעודכנת של מערכות החומרה והתוכנה של המאגר. במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יש לקיים, אחת ל-18 חודשים לפחות, סקר לאיתור סיכוני אבטחת מידע ומבדקי חדירות למערכות (penetration testing).
- **מיקור חוץ הכרוך במתן גישה למאגר המידע** – במקרה של מתן גישה למאגר מידע לנותן שירות חיצוני, יש לבחון, טרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות ולקבוע במפורש בהסכם עם הגורם החיצוני הוראות המפרטות, בין היתר, את המידע שהגורם

החיצוני רשאי לעבד, מטרות השימוש במידע, סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות, משך ההתקשרות, אופן השבת המידע או השמדתו בסיום ההתקשרות, חובתו של הגורם החיצוני להחתים את בעלי ההרשאות מטעמו על הסכם סודיות, אופן יישום חובותיו של הגורם החיצוני בתחום אבטחת המידע, חובתו של הגורם החיצוני לדווח לבעל המאגר, אחת לשנה לפחות, על אופן ביצוע חובותיו לפי התקנות וחובתו של הגורם החיצוני להודיע לבעל המאגר על אירועי אבטחה. בנוסף, התקנות מחייבות לנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בתקנות ובהוראות ההסכם עמו.

- **ביקורת תקופתית** – במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה יש לערוך, אחת ל-24 חודשים לפחות, ביקורת על-ידי גורם בעל הכשרה מתאימה (שאינו ממונה האבטחה של המאגר), על מנת לוודא את עמידתו בתקנות.
- **מיון עובדים ושיבוצם** – התקנות קובעות כי אין להעניק גישה למידע המצוי במאגר או לשנות את היקף ההרשאה שניתנה, אלא אם ננקטו אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר האם בעל ההרשאה מתאים לקבלת גישה למידע המצוי במאגר. בנוסף, התקנות קובעות כי טרם מתן גישה למידע לאדם או שינוי היקף הרשאתו, עליו לעבור הדרכה בנושא החובות לפי חוק הגנת הפרטיות ולפי התקנות. במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה יש לקיים בנוסף הדרכה תקופתית בנושא, אחת לשנתיים לפחות.
- **דיווח על אירועי אבטחה חמורים** (data breach notification) – במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או רמת האבטחה הגבוהה, קמה חובה לדווח לרשם מאגרי המידע, באופן מיידי, על כל אירוע אבטחה חמור הנוגע למידע המוחזק במאגר ועל הצעדים שננקטו בעקבותיו. הרשם רשאי, בנסיבות מסוימות, להורות לבעל מאגר המידע להודיע על אירוע האבטחה לאדם שמידע אודותיו מצוי במאגר שבו אירע אירוע האבטחה.

אמצעי אבטחה נוספים – התקנות כוללות הוראות מחייבות ביחס לאמצעים לאבטחה הפיזית של מערכות מאגר המידע, ניהול הרשאות הגישה למאגר, אמצעים לזיהוי ואימות זהותם של בעלי הרשאות הגישה, הגבלות על חיבור התקנים ניידים למערכות המאגר, הפרדה ובידוד המאגר מהאינטרנט ועוד.

התקנות צפויות להתפרסם בעת הקרובה והן ייכנסו לתוקף **בתוך שנה** מיום פרסומן.

כאמור, התקנות יחולו על קשת רחבה של חברות הפועלות בענפי המשק השונים, אשר יחויבו לנקוט שורה של צעדים בתחום אבטחת המידע. על רקע האמור, ובשים לב להיקף הדרישות החדשות ולהשפעתן על מגוון מערכים ותהליכים בחברה (IT, משאבי אנוש, רכש וכו') קיימת חשיבות רבה לנקיטת צעדי היערכות כבר בעת הזו.

צוות הסייבר, הגנת הפרטיות ואבטחת המידע של גורניצקי מציע ללקוחות גישה מקיפה ורב תחומית להתמודדות עם האתגרים המשפטיים החדשים בתחום ניהול הגנת הסייבר והגנת הפרטיות.

לפרטים נוספים:

תימור בלן (שותף)

timorb@gornitzky.com

אסף הראל (עו"ד)

assafh@gornitzky.com

45 Rothschild Blvd. Tel-Aviv 6578403, Israel | Tel: +972-3-7109191 | fax: +972-3-5606555 | www.gornitzky.com