

## המלצות להתנהלות הציבור בשימוש בעמדות טעינה לרכב חשמלי בהיבטי פרטיות

עדכון לקוחות – מרץ 2024

### לקוחות יקרים,

ביום 21.2.2024 פרסמה הרשות להגנת הפרטיות (להלן: "הרשות") מסמך שכותרתו: "המלצות להתנהלות הציבור בשימוש בעמדות טעינה לרכב חשמלי" (להלן: "המסמך"). מטרת המסמך היא להעלות את המודעות לסוגיות שיש בהן פגיעה בפרטיות המשתמשים באפליקציות המשמשות חברות המפעילות עמדות הטעינה של כלי רכב חשמליים ("אפליקציות טעינה") ומתן כלים להתנהלות מיטיבה של המשתמשים לצמצום הפגיעה הפוטנציאלית בפרטיותם.

ראינו לנכון לסקור בתמצית את עיקרי המסמך הן משום שהוא מצביע על האופן בו מומלץ למשתמשים לנהוג בעת שימוש באפליקציות, אך לא פחות מכך משום שהוא יכול ללמד על הפעולות שנכון לדעת הרשות שינקטו בהן החברות המפעילות את עמדות הטעינה ואת האפליקציות האמורות.

**נשמח לסייע לכם לבחון את ההשפעות האפשריות של המסמך על ארגונכם ואת עמידת ארגונכם בהוראות חוק הגנת הפרטיות.**

אלה עיקרי המסמך לדעתנו.

1. לפי המסמך הרשות מאפיינת שלושה מצבים עיקריים בהם נאסף מידע באמצעות עמדות הטעינה והאפליקציות הטעינה.

1.1. בזמן הרישום לשירות באפליקציה – נתונים דוגמת פרטי קשר, נתונים אודות הרכב, נתוני מיקום, פרטי אשראי ונתונים אחרים הנדרשים לשם הקמת חשבון משתמש, כגון מידע ביומטרי למי שמבקש לאפשר זיהוי לפי אמצעי זה באפליקציה.

1.2. בזמן השימוש באפליקציה - נתונים דוגמת נתוני שימוש ברשת כגון כתובת IP, היסטוריית התנהגות מקוונת ומזהי אפליקציות, וכן נתונים רגישים אחרים כגון נתוני אשראי ונתוני מיקום.

1.3. בזמן הטעינה - נתונים דוגמת שעת התחלה, שעת סיום, מזהה עמדת הטעינה, נתונים מהפרופיל וההגדרות עבור תוכנית טעינה אישית.

היקף הנתונים שנאסף, כמו גם היותם נתונים היכולים לעלות כדי מידע ואף מידע רגיש, מהווים גורם המעורר חשיפה לפגיעה בפרטיותם של משתמשי אפליקציות הטעינה ועמדות הטעינה, כפי שנפרט להלן.

2. לדעתנו הרשות מייחסת תשומת לב מיוחדת למספר מאפיינים של שירותי הטעינה במסגרת המסמך

2.1 נתוני מיקום. הרשות מגדירה במסמך "נתוני מיקום" כקואורדינטות גיאוגרפיות וחומות זמן של משתמשים, ורואה בחלקם מידע ולעיתים אף מידע רגיש. זאת משום שלשיטת הרשות, הגם שלכאורה לעיתים נתוני מיקום נאספים באופן בלתי מזוהה או משוייך לאדם כלשהו, מחקרים הראו כי באמצעות הצלבה של נתונים ניתן להתחקות אחר זהות האדם אליו משייכים נתוני המיקום. ועל כן לדעת הרשות, בנסיבות מסוימות מנתוני מיקום כשלעצמם, או בשילוב עם אינפורמציה ממקורות נוספים, ניתן להסיק מידע רגיש ביותר על אדם ופרטי מידע המוגנים לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות")<sup>1</sup>. כך למשל, הימצאותו של אדם במרפאה, העלולה להעיד על מצב בריאותו.

2.2 איסוף מידע רב. שימוש באפליקציה המספקת גישה לעמדות טעינה לרכבים חשמליים כרוך לעמדת הרשות באיסוף ובעיבוד מידע אישי רב ורגיש על אודות משתמשים, המייצר, בין היתר, "שובל דיגיטלי" של נתוני מיקום, אשר מגלויים עלול להיחשף מידע רגיש על חייו והרגליו של אדם.

2.3 גישה על ידי צדדים שלישיים רבים. הרשות מונה מספר צדדים שלישיים שלרוב מקבלים גישה למידע המעובד במסגרת השירות ולעיתים אף מסייעים באיסופו. כך למשל גופים ציבוריים כגון רשויות מקומיות, אשר במסגרת ההתקשרות שלהן עם חברות לבניית עמדות טעינה במרחב הציבורי דורשות גישה לנתונים הנאספים, גופים מסחריים המפעילים את אפליקציות הטעינה, מפתחי / יצרני האפליקציות וכן ספקי אחסון שונים. מתן גישה למידע לצדדים שלישיים, מהווה פוטנציאל לאבדן שליטה במידע ומחייב לפי דין את מקבל הגישה או המידע ובעל מאגר המידע (למשל מפעילת אפליקציית הטעינה) בביצוע פעולות מסוימות דוגמת התקשרות בהסכם לפי תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

<sup>1</sup> להרחבה אודות איסוף ועיבוד נתוני מיקום ראו גילוי דעת של הרשות להגנת הפרטיות בנושא: איסוף נתוני מיקום של עובדים באמצעות אפליקציות ומערכות איכון ברכב (יולי 2023) [בקישור](#).

3. המלצות למשתמשים. הרשות במסגרת המסמך מבקשת להביא לידיעת הציבור מספר המלצות בנוגע לשימוש מושכל באפליקציות הקשורות לעמדות הטעינה. המלצות אלה כוללות למשל בחינת השימוש שצפוי להיעשות במידע האישי של המשתמש, צמצום הרשאות הגישה של האפליקציה למיקום המשתמש, בחינת צדדים שלישיים שצפויה להיות להם גישה למידע ובהתאם לבחור את האפליקציה שהכי פחות פוגעת בפרטיות המשתמשים והקפדה על התקנת עדכוני אבטחה במשך "חיי האפליקציה".

4. מבחינת חברות המפעילות עמדות טעינה ואפליקציות נלוות, המסמך מחדד כמה דברים שחשוב לדעתנו לשים עליהם דגש במסגרת פעילות זו. כך למשל חשוב לוודא - (א) שהמסמכים להם נותן המשתמש את הסכמתו קודם לשימוש באפליקציה עומדים בהוראות הדין. ראו בהקשר זה את מזכרנו [בנושא](#) חובות יידוע והסכמה; (ב) שההסכמים עם יצרני / מפתחי האפליקציות וכן גומרים נוספים הניגשים למידע עומדים בהוראות הדין ומאפשרים למפעיל לעמוד בהוראות הדין;<sup>2</sup> (ג) שכרטיסי המאגר משקפים נכונה את הפעילות של האפליקציה; (ד) שנשמר עקרון צמידות המטרה (כך שבמידע אודות המשתמשים נעשה רק השימוש לו ניתנה הסכמתם).

המידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו. נשמח לסייע לכם לבחון את ההשפעות האפשריות של המסמך על ארגונכם ואת עמידת ארגונכם בהוראות חוק הגנת הפרטיות.

המסמך המלא זמין לקריאה [כאן](#).

<sup>2</sup> כך למשל בהקשר זה חשוב שמפעילי האפליקציות והיצרנים / המפתחים שלהם יתקשרו בהסכמי עיבוד מידע מתאימים. ראוי לשקול שמפעילים ויצרני / מפתחי אפליקציות יסדירו את נושא הגשת עדכוני אבטחת המידע של האפליקציה, כדי לוודא עמידה בהוראות סעיף 3 לעיל.

נשמח לעמוד לרשותכם בכל שאלה:



**דפנה אחיעם טל, עו"ד**

שותפה, מחלקת הייטק, טכנולוגיה והון סיכון

[dafnaa@agmon-law.co.il](mailto:dafnaa@agmon-law.co.il)



**סער רוסמן, עו"ד**

שותף, מחלקת הייטק, טכנולוגיה והון סיכון  
וראש תחום פרטיות וסייבר

[saar@agmon-law.co.il](mailto:saar@agmon-law.co.il)



**מרים שדה פישר, עו"ד**

מחלקת הייטק, טכנולוגיה והון סיכון

[miriamf@agmon-law.co.il](mailto:miriamf@agmon-law.co.il)



**הלל וייס, עו"ד**

מחלקת הייטק, טכנולוגיה והון סיכון

[hillel@agmon-law.co.il](mailto:hillel@agmon-law.co.il)