

## עקרונות לניהול סיכוני אבטחת מידע בשימוש בקוד פתוח

עדכון לקוחות – אפריל 2024

### לקוחות יקרים,

ביום 8.4.2024 פרסמה הרשות להגנת הפרטיות ("הרשות") [מסמך](#) שכותרתו "עקרונות לניהול סיכוני אבטחת מידע בשימוש בקוד פתוח" ("המסמך"). היות שהשימוש בקוד פתוח הינו פרקטיקה שכיחה, והיות שלפי הרשות היעדר מתן מענה הולם בהיבטי אבטחת מידע לסיכוני אבטחת מידע הכרוכים בשימוש בקוד פתוח, עלול לעלות לידי הפרה של הוראות חוק הגנת הפרטיות תשמ"א-1981 ("חוק הגנת הפרטיות") והתקנות שהותקנו מכוחו (על ידי בעלי המאגרים וספקי התוכנה / השירות כאחד), מצאנו לנכון לסקור את עיקרי המסמך.

אנו נשמח לעמוד לרשותכם ולסייע לארגונכם לעמוד בהוראות דיני הגנת הפרטיות ואבטחת המידע החלים עליו.

### להלן נפרט את עיקרי המסמך.

#### רקע

קוד פתוח, Open Source, הוא כינוי כללי למודל מבוסס לפיתוח תוכנה בשיתוף פעולה המוני, באופן שקוד המקור ומסמכי התיעוד זמינים באופן חופשי לציבור הרחב לשם שימוש, עריכת שינויים והפצה מחדש.

במצב דברים זה מתעורר החשש לפיו הקוד הפתוח (ששימוש בו מותנה בקבלת רישיון שימוש, אך אינו כרוך בהחזקה ברישיון מסחרי), יהיה למעשה ללא 'יצרן' אשר עומד מאחוריו, ומתחזק אותו בהיבטי אבטחה. חששות נוספים הם שקוד פתוח יפותח שלא לפי פרקטיקות פיתוח מאובטח ובקרת איכות, וכי יקשה לקיים תיעוד של רכיבים במערכות המשרתות את מאגרי המידע, המשלבות בהן קוד פתוח.

על פי המסמך, היעדר מענה הולם בהיבטי אבטחת מידע לסיכוני אבטחת מידע הכרוכים בשימוש בקוד פתוח, עלול לעלות לידי הפרה של הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו. לצורך שימוש בקוד פתוח באופן המאפשר עמידה בהוראות חוק הגנת הפרטיות והתקנות, מציינת הרשות דגשים לשימוש בקוד פתוח, ואלה העיקריים בהם לדעתנו:

1



1. פיתוח והטמעה. תקנה 5 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("תקנות אבטחת מידע") קובעת כי בעל מאגר חייב לקבוע הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר, וכן תקנה 13(ג) לתקנות אבטחת מידע, לפיה בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן; וכי לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי האבטחה שלהן, אלא אם כן ניתן מענה אבטחתי מתאים.

לפיכך, עמדת הרשות היא שאין להשתמש בספריית קוד פתוח שאינה נתמכת ומתוחזקת בידי קהילת הקוד הפתוח, או בידי גוף אחר אשר תומך בהיבטי האבטחה של הספרייה<sup>1</sup>, ו/או תוך יישום בקשות מפצות.

2. עיצוב לפרטיות ואבטחה. לדעת הרשות חשוב שסוגית הקוד הפתוח תעלה כבר במסגרת עיצוב לפרטיות, שנכון לקיים בשלבים מוקדמים של אפיון המערכת, עיצובה ופיתוחה, ובכל מקרה קודם להטמעתה.<sup>2</sup>

3. ספקים חיצוניים. סוגיות נוספות שיש לתת עליהן את הדעת לפי המסמך הן: (א) במקרה בו הקוד הפתוח משולב על ידי ספק מיקור חוץ ("גורם חיצוני"), בעל מאגר נדרש לבחון, לפני ביצוע ההתקשרות עם הגורם החיצוני, את סיכוני אבטחת המידע הכרוכים בהתקשרות ולהסדיר את נושא הפיתוח והתחזוקה של כלל המערכות שהוא מספק, לרבות רכיבי הקוד הפתוח בה;<sup>3</sup> (ב) ככל שגורם חיצוני מעוניין לתת את השירות באמצעות גורם נוסף (למשל קהילת קוד פתוח), הגורם החיצוני מחויב לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בהסכם עם בעל המאגר, ולפי תקנה 15 לתקנות אבטחת מידע.

בהקשרים אלה, היות שסעיף 17 לחוק הגנת הפרטיות קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע", דומה שעמדת הרשות היא שיייתכנו נסיבות בהן החובה לעשות שימוש זהיר ומוקפד בקוד פתוח, לא תרבוץ רק על כתפי בעלי המאגרים כי אם גם על ספקי מיקור חוץ השונים.

4. ניהול סיכונים. בכל הנוגע לניהול סיכונים הנובעים משימוש בקוד פתוח, הרשות ממליצה להיעזר במסגרות עבודה הקיימות בשוק. כמו כן, מומלץ שככל שנעשה שימוש בתוכנה קניינית או

<sup>1</sup> בנסיבות מסוימות, הדבר אף יכול להוות הפרה של האיסור לחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק, שיבוש למחשב או לחומרי המחשב.

<sup>2</sup> למזכרנו בדבר עריכת תסקיר השפעה על פרטיות, לחצו כאן.

<sup>3</sup> ראו תקנה 15(א) לתקנות אבטחת מידע. בהקשר זה, רצוי לתת את הדעת לחולשות אליהן מתייחסת הרשות בנספח הרחבה למסמך עקרונות לניהול סיכוני אבטחת מידע בשימוש בקוד פתוח.

מסחרית, יידרש הספק לאשר שהתוכנה אינה מכילה חולשות ידועות הניתנות לניצול,<sup>4</sup> וכי הוא עומד במסגרת עבודה מוכרת ומקובלת.

5. מיפוי ותיעוד. תקנה 5 לתקנות אבטחת מידע קובעת כי על בעל מאגר מידע למפות את מבנה מאגר המידע, ולהחזיק רשימת מלאי מעודכנת של מערכות המאגר, לרבות תוכנות וממשקים. לשם כך, לדעת הרשות, על בעל המאגר: (א) לזהות רכיבי תוכנה בקוד פתוח הנמצאים בשימוש (כולל אלו הנמצאים בשימוש עקיף); (ב) לקבוע ולנהל באיזה רישיון משתמש כל רכיב קוד פתוח; (ג) להגדיר ולנהל את נוהלי הקוד הפתוח ולוודא שהתחייבויות הרישוי מתקיימות בעת השימוש או בעת שחרור מוצר; (ד) לוודא סקירה כללית של תוכנית תאימות לקוד פתוח; (ה) להקפיד על ביצוע הכשרה של כלל המעורבים בפיתוח ובניהול הקוד על פי הנדרש. בהקשר זה מציינת הרשות כלים ארגוניים, שלדעתה יכולים לסייע לבעל המאגר לעמוד בחובות אלה.

**נשמח לסייע לארגונכם לעמוד בהוראות והמלצות המסמך ולוודא עמידה בהוראות הגנת הפרטיות ואבטחת המידע החלות עליו.**  
לקריאת המסמך המלא יש לחוץ [כאן](#).

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.

<sup>4</sup> Known Exploitable Vulnerabilities.

נשמח לעמוד לרשותכם בכל שאלה או התייעצות:



עו"ד הלל וייס

מחלקת הייטק, טכנולוגיה והון סיכון  
hillel@agmon-law.co.il



עו"ד סער רוסמן, שותף

מחלקת הייטק טכנולוגיה והון סיכון,  
ראש תחום סייבר ופרטיות  
saar@agmon-law.co.il



עו"ד מרים שדה פישר

מחלקת הייטק טכנולוגיה והון סיכון  
צוות סייבר ופרטיות  
miriamf@agmon-law.co.il