



23 מרץ 2020
כ"ז אדר תש"פ

הגנת הפרטיות בעקבות התפשטות נגיף הקורונה: שאלות ותשובות להתנהלות הציבור, גופים ציבוריים והשוק הפרטי

רקע

ימים מורכבים עוברים על כולנו. הניסיון למנוע את התפשטות נגיף הקורונה, והחשש מפני התפשטות זו, משפיעים באופן דרמטי על ההתנהלות וחיי היומיום של כל אחת ואחד מאתנו. משרדי הממשלה השונים, כמו גם ארגונים ציבוריים אחרים, נוקטים בצעדים משמעותיים בכדי להכיל את התפשטות הנגיף ובכדי להפחית את השלכותיו. רשויות המדינה עורכות הערכות מצב ומפרסמות הנחיות שונות הבאות להסדיר את התנהלות הציבור בהיבטים שונים, לרבות התקנת תקנות לשעת חירום.

מבין הדברים יש לשים לב להשפעה של מצב חירום זה על היבטי הפרטיות. הזכות החוקית לפרטיות, חוק הגנת הפרטיות, התשמ"א-1981 והתקנות הנגזרות ממנו, אינם עומדים בדרכם של שירותי הבריאות וגופים נוספים בבואם למנוע את התפשטות הנגיף ואינם מונעים במקרה זה, את ניהול בריאות הציבור. עם זאת, ישנם שיקולים חשובים אותם יש לקחת בחשבון בעת טיפול במידע אישי בהקשרים אלה, ובמיוחד מידע רגיש כזה או אחר, ועל מנת לבצע את האיזונים הנדרשים בטיפול במקרים השונים.

הרשות להגנת הפרטיות מבינה את האינטרס הציבורי הרחב במצב החירום הנוכחי, מזהה את האתגרים העומדים בפנינו ותייעץ ככל הנדרש בנושאים שבתחום אחריותה. **מטרת מסמך זה הינה להציג לציבור, לגופים ציבוריים ולגורמים פרטיים (ובראשם מעסיקים) דגשים להגנת פרטיות במצב זה.**

הרשות להגנת הפרטיות הקימה "קו חם" לסיוע במתן פתרונות מעשיים, ישימים ומהירים בתחומי פרטיות, וצוות הרשות זמין בכל עת למתן פתרונות בנושאי פרטיות ועיצוב פתרונות תומכי פרטיות בכל נושא הרלוונטי לפעילות החירום בעת הזו. יודגש כי פתרונות ישימים אלה יינתנו על ידי הרשות בלוחות זמנים קצרים ביותר כמתבקש בנסיבות.

ניתן לעמוד עמנו בקשר דרך עמוד הפייסבוק של הרשות ("הרשות להגנת הפרטיות") או במייל: ppa@justice.gov.il
נשמח לעמוד לרשותכם בכל נושא ועניין ולספק מענה לשאלותיכם.





כללי

הזכות לפרטיות היא זכות יסוד חוקתית אשר נקבעה בחוק-יסוד: כבוד האדם וחירותו. סעיף 7 לחוק היסוד קובע, בין השאר, כי "כל אדם זכאי לפרטיות ולצנעת חייו". נוסף על מעמדה של הזכות לפרטיות כזכות יסוד חוקתית, נהנתה הזכות עוד לפני חקיקת חוק היסוד, להגנה מפורשת ונרחבת בחוק הגנת הפרטיות, התשמ"א-1981. החוק חל הן על המגזר הציבורי והן על המגזר הפרטי, והוא קובע כי פגיעה בפרטיות תהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית שעונשה חמש שנות מאסר.

אחד מעקרונות הבסיס של החוק הוא דרישת ההסכמה. החוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק לא מגדיר מהי הסכמה אלא רק מציין כי הסכמה צריכה להיות מדעת, ולהינתן במפורש או במכללא. ברמה העקרונית, הכלל הוא שאין לאסוף מידע על אדם אלא אם הוא מודע שמידע נאסף אודותיו, הוא מסכים לאיסוף המידע וכן מסכים לשימושים השונים שאוסף המידע מבקש לעשות בו.

עם זאת, הזכות לפרטיות אינה זכות מוחלטת. מבחינה חוקתית, לרשויות המדינה יש סמכות לפעול באופן שיש בו בכדי פגיעה בפרטיות הציבור (כולו או חלקו), כל עוד הן פועלות בהקשר זה מתוקף הסמכה מפורשת בהוראות הדין, המאפשרת פעילות שכזו, לתכלית ראויה ובמידה שלא עולה על הנדרש. גם חוק הגנת הפרטיות מכיר בנסיבות יוצאות דופן בהן ניתן לפעול באופן הפוגע בפרטיות, וזאת מתוקף ההגנות שבהוראות סעיף 18 לחוק. כך לדוגמה, סעיף 18 (2) (ב) לחוק קובע כי במקרה בו פגיעה בפרטיותו של אדם נעשתה בתום לב ובנסיבות בהן הייתה על הפוגע "חובה חוקית, מוסרית, חברתית או מקצועית לעשותה", הרי שאותו אדם יהיה מוגן מפני הסנקציות הקבועות בחוק. ובדומה, סעיף 18 (3) קובע כי הגנה שכזו תעמוד במידה ובפגיעה היה עניין ציבורי המצדיק אותה בנסיבות העניין.

יודגש כי האפשרות להסתייע בהגנות סעיף 18 לפטור מאחריות בגין פגיעה באחריות מותנית בקיומה של סיטואציית חירום אשר מונעת בפועל את האפשרות להסדיר את השימוש במידע באופן חוקי, למשל על ידי קבלת הסכמה מנושא המידע, הסמכה בחיקוק או העברת מידע לפי פרק ד' לחוק הגנת הפרטיות. במילים אחרות הגנת סעיף 18 היא רק בדיעבד ולא מלכתחילה, וכשתסתיים שעת החירום הנובעת ממגפת הקורונה לא ניתן יהיה עוד להסתמך בתום על הגנת סעיף 18.

משמעות הדבר היא שבנסיבות מסוימות, פגיעה בפרטיות עשויה להיחשב מוצדקת, וככזו היא תהיה מוגנת מבחינת הוראות הדין. ואולם, גם כאשר קיימת לגופים מדינתיים ופרטיים האפשרות לפעול באופן הפוגע בפרטיות הציבור, אין בדברים בכדי לומר כי גופים אלו רשאים לעשות כן ללא התחשבות במשמעות פעילותם מבחינת הפגיעה בפרטיות הציבור.

מצבי קיצון והניסיון להתמודד עם השלכות מצבים אלו עשויים, במקרים מסוימים, לחייב גופים מדינתיים ופרטיים לפעול באופן העשוי לפגוע בפרטיותו של אדם, וזאת מבלי לקבל את הסכמתו





לכך. הצורך להציל חיי אדם, וביחס לנסיבות הנוכחיות - למנוע את התפשטות נגיף הקורונה - עשויים בהחלט להצדיק נקיטת פעילויות מסוימות מצדם של גופים ציבוריים ופרטיים שיש בהן בכדי לפגוע בפרטיות.

עם זאת, עמדת הרשות להגנת הפרטיות היא כי גם במצבי חירום, כאשר קיימת הצדקה לכאורה לפגיעה בפרטיות כלל הציבור או חלקים ממנו, יש להקפיד לפעול בהתאם לעקרונות ההגנה על פרטיות, ועל כך שהפגיעה הנגרמת כתוצאה מהפעילות לא חורגת מהנדרש בנסיבות העניין.

עקרון מרכזי הוא שימוש במידע אך ורק למטרה שלשמה הוא נאסף. הטיפול בהתפשטות נגיף הקורונה והניסיון להביא לצמצום התפשטות זו, יוצרים מצב בו מידע רב אודות פרטים נאסף ונאגר במאגרי מידע שונים. על הגופים השונים האוספים מידע במסגרת האמורה, להשתמש בו אך ורק למטרה שלשמה הוא נאסף, כדוגמת מניעת התפשטות הנגיף, מחקר אפידמיולוגי, הבטחת שלומם של עובדים בסיכון וכיוצא בזה. שימוש במידע (כדוגמת עיבודו או העברתו לגופים אחרים) שלא למטרה שלשמה הוא נאסף מלכתחילה, וללא קבלת הסמכת נשוא המידע לשימוש זה, עשויה על-פניו להיחשב כפגיעה בפרטיות, ועל הגופים הרלוונטיים להימנע מכך.

במובן זה, לאחר סיומו של התהליך, על הגופים השונים לבחון את הצורך בהמשך החזקת המידע. בנסיבות בהן יימצא כי אין עוד צורך בהחזקת ושמירת המידע, מומלץ להביא למחיקתו. ראו בעניין זה, למשל, את סעיף 2(ג) לתקנות הגנת הפרטיות (אבטחת המידע), התשע"ז-2017, הקובע כי "בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר". ככל שמדובר במידע רגיש על אודות פרטים, וככל שאין עוד צורך בשמירתו, על הגופים האוספים את המידע לבחון אפשרות למחוק המידע תוך פרקי הזמן הקצרים ביותר האפשריים בנסיבות העניין.

להלן יוצגו מספר שאלות ותשובות הנוגעות להתנהגות במסגרת טיפול בהתפשטות נגיף הקורונה.

שאלות ותשובות

האם מעסיקים רשאים לדווח לעובדים או למבקרים במקום העבודה על כך שאחד העובדים עמו הם היו בקשר חלה בנגיף (או שיש חשש כי הוא נשא שלו)?

כן. ברמה העקרונית ועל יסוד הוראות סעיף 18 שפורטו קודם לכן, יידוע עובדים ו/או גורמים אחרים על חשש להידבקות של עובד עמו הם היו בקשר בתקופה הרלוונטית עשוי להיחשב מוצדק, כל עוד יידוע זה נעשה בתום לב.

עם זאת, על מעסיקים להקפיד לדווח רק על המידע הרלוונטי בנסיבות העניין ולא להעביר מידע שאינו הכרחי לשם היידוע, כגון מידע אישי ופרטי אודות העובד. כך, ככל שאפשר לדווח על חשש להידבקות על יסוד הימצאות באזור ובזמן מסוימים בהם שהה העובד, תוך אי-אזכור פרטי המזהים, על מעסיקים להקפיד שלא לדווח ולחשוף פרטים אלו.



כמו כן, על מעסיקים להקפיד ככל האפשר להעביר את המידע רק לגורמים הרלוונטיים. על מעסיקים לנסות ולהימנע מלחשוף ולפרסם מידע אודות עובדים בהקשר זה לכלל הציבור, אלא רק לגורמים הספציפיים אשר, למיטב ידיעת המעסיקים, היו בקשר עם העובד הרלוונטי. ככל שפרסום נקודתי שזוה אינו אפשרי, הרי שמעסיקים יהיו רשאים לפרסם את המידע במעגלי דיווח רחבים יותר.

האם גופים ציבוריים יכולים להעביר ביניהם מידע לשם מתן שירותים במסגרת ההתמודדות עם התפשטות נגיף הקורונה?

כן. בידי רשויות המדינה מידע רב על אזרחים, הנוגע לכל היבטי חייהם. שיתוף מידע אישי אודות אנשים בין גופים ציבוריים שונים הוא כלי חשוב לייעול השירות שניתן לציבור ולהקלת הנטל הבירוקרטי. יחד עם זאת, העברת מידע אישי בין גופים עשויה להשליך על הפרטיות של אותם אנשים ולכן יש צורך בקביעת מנגנונים ייחודיים להגנה על המידע האישי המועבר.

העברת מידע בין גופים ציבוריים מותרת במסגרת תנאי פרק ד' לחוק הגנת הפרטיות. העברת מידע בין גופים ציבוריים שלא במסגרת כך מהווה עבירה פלילית. סדרי העברת מידע בין גופים ציבוריים הוסדרו בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986. תקנות אלה כוללות את הדרישות הבאות בכל מקרה בו גוף ציבורי מעוניין או נדרש להעביר מידע אל גוף ציבורי אחר.

באופן כללי, על מנת להעביר מידע בין גופים ציבוריים, יש לבחון את מידתיות וסבירות הבקשה בהתייחס לרגישות המידע אותו מעוניינים להעביר. ככל שהמידע רגיש יותר יש צורך בהגנה רבה יותר על הפרטיות, תוך בחינת האלמנטים הבאים:

- האם הבקשה מתאימה ליישום המטרה לשמה נדרש המידע ויש קשר הגיוני ביניהן.
 - האם העברת המידע באופן המבוקש היא אמצעי פחות פוגע מבין מגוון האמצעים למימוש אותה המטרה.
 - האם קיים יחס סביר בין המטרה לבין הפגיעה שנגרמת בזכות לפרטיות לשם השגתה.
- בחינת מידתיות וסבירות הבקשה להעברת המידע כמו גם המבחנים שפורטו לעיל מיושמים על פי נסיבותיו של כל מקרה ומקרה. סביר להניח כי במצבי חירום, כדוגמת המצב הנוכחי, המחייבים העברת מידע מהירה בין גופים ציבוריים לקידום והגנה של אינטרסים ציבוריים ראויים, ייטה האיזון בין מטרת העברת המידע לפגיעה העשויה להיגרם מכך, לכיוון מתן האפשרות של גופים להעביר מידע ביניהם, וזאת, בין היתר, בהתאם להוראות סעיף 18 לחוק הגנת הפרטיות.



כמו כן על הגורם המעביר את המידע לבחון את סוגיית אבטחת המידע של מאגר המידע בגוף המקבל את המידע. להרחבה ראו מדריך העברת מידע בין גופים ציבוריים באתר הרשות:

https://www.gov.il/BlobFolder/service/information_flow_between_public_bodies/he/info-bulletin.pdf

האם יש היבטי פרטיות שיש להיות מודעים אליהם במסגרת של עבודה או למידה מרחוק?

כן. כחלק מהניסיון למנוע ולצמצם את התפשטות נגיף הקורונה התבקשו עובדים, סטודנטים ותלמידים לעבוד וללמוד מביתם. העברת פעילות פרטים מהמרחב הציבורי לפרטי היא מתבקשת בסיטואציות של התפרצות מגיפות ונגיפים. עם זאת, יש לזכור כי מערכות טכנולוגיות המאפשרות עבודה ולמידה מרחוק הן ברובן מערכות האוספות מידע על משתמשים, לרבות מידע רגיש. מערכות אלו גם אינן חסינות מפני חדירה ומפני מצבים של דלף מידע. לאור האמור, על מקומות עבודה, מוסדות חינוך ומוסדות אקדמיים להקפיד על ביצוע כל הפעולות הנדרשות מבחינת אבטחת מידע וזאת על מנת לאפשר פעילות בטוחה לכל מי שמתבקש לעבוד וללמוד מביתו.

הרשות להגנת הפרטיות מבקשת להפנות בעניין זה לממצאי פיקוח רחב שערכה בקרב גופים המנהלים פלטפורמות לימודיות וחינוכיות לקטינים. ממצאים אלו מלמדים על החובה המוטלת על הגופים הרלוונטיים לפעול בעניין באופן שמבטיח את פעילותם של תלמידים, בעיקר בעתות משבר וחירום בהם כמות גדולה מהם פועלת במסגרת מערכות למידה מרחוק.

לעיון בדו"ח הרשות ראו:

https://www.gov.il/BlobFolder/news/website_platforms_and_learning_apps/he/Minor%20report.pdf

איך אפשר להגן על מידע אישי של עובדים/סטודנטים/תלמידים הפועלים מרחוק?

באופן כללי, על מעסיקים לבחון כי הם עומדים בהוראות תקנות הגנת הפרטיות (אבטחת המידע), התשע"ז-2017. בעידן המידע, אבטחת מידע היא חלק אינטגרלי ומשמעותי בהגנה על פרטיות. הרשות להגנת הפרטיות מכירה בכך שמצבי חירום, כדוגמת המצב הנוכחי, מחייבים את הגופים השונים לפעול במהירות, וכי לחובה זו עשויה להיות גם השלכה על סוגיות של פרטיות. עם זאת הרשות מבקשת להבהיר כי בכל הנוגע להיבטים של אבטחת מידע, אין במצב חירום בכדי להצדיק אי עמידה של הגופים השונים בהוראות הדין הרלוונטיות לעניין זה.

להלן מספר הצעות להגנה על מידע בזמן עבודה ולמידה מרחוק:

- הקפידו לעבוד רק עם אמצעים טכנולוגיים ייעודיים ולהימנע ככל האפשר מפעילות עם אמצעים "חינמיים" הפתוחים לכלל הציבור, כגון חשבונות Gmail. במידה ונאלצים





להשתמש בכלי דואר אלקטרוני פרטיים רצוי להגביר את תשומת הלב ולבדוק היטב את הנמענים ואת התוכן המועבר כדי להימנע מיצירתו של אירוע אבטחה בעקבות טעות אנוש במסגרתה נשלח מידע רגיש אל מחוץ לארגון.

- הקפידו כי האמצעים הטכנולוגיים שברשותכם (לרבות מערכות ההפעלה עמן אתם עובדים) מעודכנים וכי בכולם פועלות תוכנות להגנה על מידע כגון תוכנות של חומת אש, אנטי-וירוס וכדומה.

- רצוי להשתמש רק בסיסמאות חזקות למחשב ולשירותים השונים בהם נעשה שימוש. סיסמה חזקה היא כזו אשר תקשה על ניחוושה ותכלול תווים רבים ככל האפשר (8 תווים מינימום ועדיף יותר), שילוב של אותיות קטנות, אותיות גדולות, מספרים ותווים מיוחדים נוספים. זכרו להשתמש בסיסמאות שונות לשירותים שונים על מנת להימנע ממצב בו חשיפה של סיסמא אחת תאפשר פגיעה ביתר השירותים.

- נקטו בהליכי הגנה כגון אימות דו-שלבי ל"כניסה" ושימוש בכלי ואמצעי עבודה מרחוק.

- הימנעו מכניסה לאתרים לא מורשים בעת עבודה או למידה מרחוק.

- גבו את תוצרי העבודה שלכם ביחידות אחסון שאינן פועלות ברשת, כגון כוננים ניידים (גיבוי קר).

בהתאם להודעת מערך הסייבר הלאומי בעניין זה, הרשות להגנת הפרטיות מבקשת להדגיש כי עם העלאת המודעות בדבר נגיף הקורונה והתפשטותו בעולם, נרשמה עלייה במספר הניסיונות לביצוע מתקפות סייבר של גופים שונים, בין היתר באמצעות כלים של הנדסה חברתית. מצב עניינים זה מחייב מעסיקים, כמו גם את הציבור הרחב, ביישום כללי זהירות שונים.

להלן מספר כללי אצבע להתגוננות אישית:

1. שימו לב לזהות שולח ההודעה ולקשר שלו לתוכן ההודעה. אם אינכם מכירים את השולח - השתדלו לא לפתוח את המייל במידת האפשר, ובוודאי שאין לפתוח צרופות המצורפות להודעה או להקיש על הקישורים הכלולים בה.

2. חפשו סימנים חשודים:

- גורם המבקש מכם לשלוח פרטים אישיים כאשר הוא אמור לדעת פרטים אלה;
- ניסיונות להלחיץ באמצעות מצג שווה למצב חרום, סנקציה או מועד אחרון להגשה;
- תוכן וסגנון ההודעה נראה חובבני, כולל טעויות כתיב, תחביר רעוע או תחביר שאינו מתאים לתוכן המכתב (למשל: מכתב מבנק אשר נשלח מתיבת Gmail).

3. קישורים לאתרים או גופים הנשלחים אליכם פתחו בנפרד בהקלדה יזומה בדפדפן.

4. אם קיבלתם הודעה חשודה המבקשת לעדכן פרטי תשלום, לפתוח חשבון שנחסם ועוד - צרו קשר ישירות מול החברה השולחת לכאורה.





5. זכרו כי פרטי המשתמש שלכם קבועים עד אשר מיוזמתכם אתם מבצעים שינוי, אף מוסד פיננסי או ארגון וגם לא מערכות מידע והתמיכה לא יבקש את פרטיכם האישיים, אלא יבצעו את השינוי במסגרת אתר החברה ואחרי שביצעתם הזדהות.

להרחבה ראו הנחיות מערך הסייבר הלאומי בעניין זה:

<https://www.gov.il/BlobFolder/reports/corona-virus-alert/he/CORONA-CERT-IL-W-1026.pdf>

האם לאנשים עליהם נאסף מידע לאור התפשטות הנגיף יש זכויות מסוימות במידע זה?

כן. על-פי חוק הגנת הפרטיות, לנושאי מידע קיימות מספר זכויות הנוגעות לאופן השימוש במידע הנוגע אליהם. כך, פנייה לאדם לקבלת מידע על אודותיו לשם החזקתו או שימוש בו במאגר מידע חייבת לכלול הסבר האם מסירת המידע היא ברשות או בחובה, ציון המטרה אשר לשמה מבוקש המידע וכן פירוט למי יימסר המידע, ולשם מה.

כמו כן, חוק הגנת הפרטיות קובע כי ככלל, לכל אדם עומדת הזכות לעיין במידע הנוגע אליו ואשר מוחזק במאגר מידע מסוים. החוק קובע כי במידה ואדם מוצא שהמידע עליו אינו שלם, מדויק או מעודכן, הרי שעומדת לו הזכות לדרוש את תיקון המידע או את מחיקתו.

על גופים האוספים מידע על אודות פרטים כחלק מפעילותם למניעת התפשטות נגיף הקורונה להקפיד על עמידה בהוראות החוק בכל הנוגע לזכויות נושאי המידע, לרבות אלו שפורטו לעיל.

הרשות להגנת הפרטיות מכירה בכך שבעתות משבר וחירום ייתכן קושי מסוים לעמוד בכללים האמורים. עם זאת, על הגופים הרלוונטיים להיערך לצורך לעמוד בכללים אלו. בכל הנוגע לאכיפת זכות העיון במידע, הרשות תתחשב במועד קיומה בתקופות משבר וחירום ולאור האתגרים הקיימים בתקופות אלו.

סיכום

אנו נמצאים בעיצומה של תקופה מורכבת. הניסיונות להתמודד עם התפשטות נגיף הקורונה והשלכותיה עשויים להשפיע גם על פרטיותנו ועל ההגנה על מידע הנוגע אלינו. לפיכך, על גופים ציבוריים, מעסיקים ועל הציבור בכללותו לפעול בעניין באחריות ותוך הקפדה על עקרונות הגנת הפרטיות וההגנה על המידע.

לשאלות והרחבות בעניינים אלו ואחרים בקרו באתר האינטרנט של הרשות להגנת הפרטיות:

https://www.gov.il/he/departments/the_privacy_protection_authority

