

תקציר מנהלים: פרטיות בחירום

גם בעתות חירום, **חוק הגנת הפרטיות אינו מושעה**. ניהול מאגרי מידע, ניטור עובדים ושימוש במידע אישי מחייבים איזון קפדני בין צרכי החירום ודרישות גורמי הביטחון, לבין עקרון המידתיות.

במדינת ישראל, האיזון בין צרכי הביטחון וההתמודדות עם מצבי חירום, לבין שמירה על הזכות החוקתית לפרטיות – מרכזיים ונוכחים תמיד. הרשות להגנת הפרטיות פרסמה ביום 18/9/2024 (ועדכנה ביום 13/8/2025) מסמך מדיניות מקיף העוסק בהגנה על פרטיות בתקופות חירום, תוך הדגשת הקווים המנחים שצריכים להנחות רשויות וגופים ציבוריים ופרטיים גם בעיתות משבר. המסמך מתכתב באופן ישיר עם תיקון 13 לחוק הגנת הפרטיות, התשמ"א-1981, ומבסס לראשונה מנגנוני אכיפה וסנקציות משמעותיים. בכך הוא יוצר מדריך מעשי לארגונים, ומחדד את האחריות המשפטית להבטחת פרטיות גם כשהנסיבות דורשות תגובה מהירה וחריגה. סקירה.

מה העקרונות המרכזיים בהגנת הפרטיות בשעת חירום?

הסכמה מדעת: כלל בסיסי בשגרה ובחירום

העיקרון הראשון שמדגישה הרשות הוא **עקרון ההסכמה**. גם בשעת חירום, נקודת המוצא היא כי שימוש במידע אישי מחייב הסכמת נושא המידע או הסכמה מפורשת בחוק. חריגה מכך תתאפשר רק כאשר מתקיים צורך חיוני מובהק, ובנסיבות שלא ניתן לקבל בהן הסכמה סבירה. בכך משמרת הרשות את מעמד הזכות לפרטיות כזכות יסוד, שלא ניתן להפקיעה אלא בהתאם לדרישות החוק והמידתיות. הדוגמאות מהעבר, ובראשן השימוש באמצעי מעקב טכנולוגיים בתקופת הקורונה, ממחישות את הצורך בהצבת גבולות ברורים. החלטות שהתקבלו אז תחת לחץ זמן עוררו ביקורת ציבורית ומשפטית, והדגישו כי פגיעה רחבת היקף בפרטיות עלולה לערער אמון הציבור ברשויות גם בשגרה.

חובת יידוע – גם בדיעבד

חוק הגנת הפרטיות והפסיקה הישראלית קבעו כי איסוף מידע אישי מחייב, כעיקרון יסוד, מתן יידוע מוקדם לנושא המידע באשר למטרות השימוש במידע, לזהות האחראי על העיבוד, לזכויות הנתונות לו ולפרטי יצירת הקשר עם מחזיק המאגר. מטרת החובה היא לאפשר שקיפות והגברת שליטת הפרט במידע האישי שלו.

אלא שבשעת חירום (מתקפת סייבר, אירוע ביטחוני רחב היקף, מגיפה וכיוצ"ב) – פעמים רבות לא מתאפשר לקיים את חובת היידוע בזמן אמת. לדוגמה, כאשר נדרש איסוף מיידי של נתוני מיקום או בריאות לצורך הצלת חיים, אין אפשרות מעשית לפנות לכל נושא מידע ולקבל את הסכמתו המודעת תוך יידוע מלא. עם זאת, הרשות מדגישה כי מצב זה **אינו מעניק לגורם האוסף פטור מחובת היידוע**. לכל היותר, ניתן לדחות את מועד קיום החובה, אך לא לוותר עליה כליל.

במילים אחרות, גם אם השיקולים המבצעיים והלחץ התפעולי מונעים יידוע מיידי, הרי שמיד עם חלוף הסכנה המיידית או עם התייצבות המצב, על הגוף האוסף להשלים את החובה ולהודיע לנושאי המידע על עצם האיסוף,

טופס 11 – תיעוד העברת מידע במצב חירום

מטרותיו והיקפו. בכך נשמרת הליבה של הזכות לפרטיות - ההכרה בזכותו של אדם לדעת כי מידע אודותיו נאסף, ולעמוד על זכויותיו כלפי המחזיק במידע.

עיקרון זה מגלם מחויבות כפולה: מצד אחד, הכרה במציאות הקשה של מצבי חירום והצורך בגמישות מבצעית. מצד שני, שמירה על אמון הציבור ועל תוקפה של חובת השקיפות גם בזמנים יוצאי דופן. הרשות אף מדגישה כי רק במקרים קיצוניים, בהם קיימת מניעה מוחלטת ליידוע במועדו, ניתן להצדיק דחייה בהשלמת החובה. גם אז, יש להוכיח כי נעשה כל מאמץ למזער את הפגיעה בזכויות הפרט.

עקרון צמצום המידע

רשות או גוף פרטי האוסף מידע אישי בתקופת חירום נדרש להפעיל עקרון צמצום מידע. יש לאסוף אך ורק את המידע הדרוש לצורך ההתמודדות עם האירוע, ולהימנע מהשאת מידע במאגרים מעבר לנדרש. לאחר החזרה לשגרה, יש לבצע בחינה יזומה **ולמחוק מידע שהפך לעודף**. מסר זה חשוב במיוחד לאור תיקון 13, אשר קובע חובות מוגברות לעניין ניהול מאגרי מידע והערכת סיכונים.

אבטחת מידע מוגברת

בעתות חירום מתרבים ניסיונות תקיפת סייבר מצד גורמים עוינים, ובמיוחד כאשר מערכות המדינה נתונות בלחץ. מסמך הרשות קובע כי דווקא אז יש להקפיד הקפדה יתרה על דרישות תקנות אבטחת המידע. ארגונים נדרשים להכין מראש תרחישי חירום, לוודא חוסן טכנולוגי, ולאמץ נוהלי תגובה מהירה לאירועי אבטחת מידע. היערכות מוקדמת היא מפתח להפחתת סיכונים.

מידע על נפטרים – רגישות כפולה

סוגיה ייחודית שהועלתה במסמך נוגעת למידע אישי של נפטרים. אף שאין לנפטר עצמו זכות לפרטיות, הרי שהמידע עשוי לכלול פרטים על בני משפחתו או על צדדים שלישיים שהיו עמו בקשר. הרשות מדגישה כי יש לנהוג בזהירות יתרה בשאלת מסירת מידע לבני משפחה או פרסום פרטים לציבור, תוך ניסיון לכבד את רצונו המשווער של הנפטר ואת פרטיות המעורבים.

עקרונות מידתיות וצמידות המטרה

הקו המנחה לאורך המסמך הוא עקרון המידתיות. שימוש באמצעי הפוגע בפרטיות עשוי להיות מוצדק במצב חירום – אך אין לראות בכך היתר גורף. מה שנחשב מידתי בזמן חירום אינו לגיטימי בהכרח בשגרה או בתקופת "שגרת חירום". לפיכך יש לקבוע מנגנוני בקרה ברורים להפסקת השימוש באמצעים הפוגעניים עם תום מצב החירום.

פרטיות בניהול מידע: שגרה מול סיכון וחירום



ניהול שגרה

בשגרה, הדגש הוא על ציות מובנה (Privacy by Design), הסכמה מדעת ושמידה על עקרונות יסוד תחת נהלי אבטחה מותאמים.

בחירום, הדדושות הרגולטוריות החפכות (ftraw en Design) ממרחונית יחשש שכלים פולשנים (כמו ניתוח AI) יישארו בשימוש קבוע ללא הצדקה.

ארגוני

איש

נושא

משולש החשיפה

68% מהנופים נכשלו בביצוע בקורות נאותות על ספקי מיקור חוץ (ממצאי פיקוח רוחב).

דגשים לניהול סיכונים וחירום

חובת מינוי DPO:
במצבים של עיבוד מידע רגיש נרחב או מעקב שיטתי, תיקון 13 מחייב מינוי ממונה רשמי.

בקרה על גורמי חוץ (מיקור חוץ):
בעת התקשרות עם ספק, חובה לחתום על הסכם DPA הכולל הנחיות אבטחה, דיווח שנתי ומחיקת מידע.

מפת דרכים ליישום בטוח

- ✓ **בחנית צורך:** הערכת הצורך העסקי והצדקת איסוף המידע.
- ✓ **צמצום שדות:** הסרת שדות מידע שאינם חיוניים.
- ✓ **הסכם DPA:** חתימה על הסכם הגנת מידע עם כל ספק מיקור חוץ.
- ✓ **בקרה:** ביצוע ביקורות וסקרי סיכונים תקופתיים.

מצבי סיכון וחירום



בחירום, הדדושות הרגולטוריות הפכות לקשיחות ואינטנסיביות יותר, עם חובות דיווח מידיות ובקורות פולשניות למניעת נזק.

פרטיות בעת שגרה	פרטיות בעת סיכון / אירוע אבטחה	
איוון אינטרסים	עדיפות עליונה להגנה על המידע וצמצום נזקים, גם במחיר פגיעה זמנית בנוחות.	⚖️
עיקרון ההסכמה	הפעולות נגזרות מהחוק (חובת דיווח) ולא מהסכמת המשתמש.	✅
חובת הידוע	חובת דיווח מיידית לרשם מאגרי המידע/ רבולטור (תוך 72 שעות ב-GDPR)	📧
מידתיות	נקיטת כל אמצעי נדרש לבלימת האירוע, תוך מידור גישה לטרימי הטיפול.	📏
צמצום מידע	שימוש במידע לחקירת האירוע, הדרהמשיכה.	🎯
צמצום מידע	שימוש במידע לחקירת האירוע, התאוששות ואבטחה (חריגה מבוקרת).	🔍
אבטחת מידע	מניעת אונרת נתונים עודפים שמגדילים את "שטח הפנים" של הסיכון.	🔒
גרמול	סקרי סיכונים ומבדקי חדירה כל 1.5 שנים (מאגרים גבוהים); דיון רבעוני באירועי אבטחה.	🕒
עיקרון המידע	חשש שכלים פולשניים (כמו ניתוח AI) יישארו בשימוש קבוע ללא הצדקה.	🔒

NotebookLM

מתי חובה לדווח על אירוע אבטחה בחירום?

מצב חירום אינו מעניק לארגונים פטור מחובות הדיווח הקבועות בדין. על פי תיקון 13 לחוק הגנת הפרטיות, חובת הדיווח על אירועי אבטחת מידע חמורים נותרת שרירה וקיימת גם בעתות משבר. עם זאת, יישום החובות דורש רגישות משפטית מיוחדת, תוך איזון בין אילוצי המצב לבין השמירה על זכויות הנושאים במידע, בהתאם להנחיות המעודכנות והקפדניות של הרשות להגנת הפרטיות.

צ'ק-ליסט דיווח מהיר: ניהול אירוע אבטחת מידע וסייבר בארגון



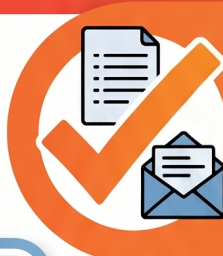
1. זיהוי ובידוד (עצירת זליגה)

זיהוי מקור הפריצה וביצוע פעולות טכניות מיידיות לעצירת הדלף, כגון ניתוק מערכות או חסימת גישות לא מורשות.



2. סיווג האירוע

בחינה האם מדובר ב"אירוע אבטחה חמור" לפי התקנות (למשל: שימוש במידע ללא הרשאה או פגיעה בשלמותו במאגר ברמת אבטחה גבוהה).



3. דיווח פורמלי לרשות להגנת הפרטיות

חובת דיווח מיידית (ועד 72 שעות לכל המאוחר) בצירוף תיאור האירוע, סוג המידע שנחשף והצעדים שננקטו.



פינת המומחה: אחריות מנהלים



הערת מומחה: עו"ד רועי וולר:
"דיווח בזמן ופעולה בתום לב הם המגן הטוב ביותר של המנכ"ל. היעדר דיווח או הסתרה עלולים להוביל להטלת אחריות אישית על נושאי משרה."

מניעת אחריות אישית: פיקוח אקטיבי על ספקים ודיווח שקוף לרשויות מצמצמים את החשיפה לתביעות אזרחיות ועיצומים כספיים.



4. גיבוש תוכנית יידוע

הערכת הצורך והדרך להודיע לאנשים שהמידע שלהם נחשף, בהתאם לחומרת האירוע ולדרישות הרשם.

מסקנות והערכות לעתיד

האחריות במיקור חוץ היא שלכם
גם אם המידע נפרץ בשרתי הענן של הספק, הישירים לאבטחת המידע ולדיווח.



חובת ה-DPA
הקפידו על הסכם עיבוד נתונים (DPA) חתום מול כל ספק, הכולל חובת דיווח של הספק אליכם תוך 24 שעות.



תרבות של "תום לב"
ארגון שמנהל יומן אירועים (Log) ומבצע הדרכות עובדים יוכל להוכיח שעמד בחובותיו גם במקרה של פריצה.



טופס 11 – תיעוד העברת מידע במצב חירום

לארגונים ציבוריים ופרטיים מומלץ לנקוט במספר צעדים מעשיים:

- **גיבוש נהלי חירום לפרטיות** - לקבוע מראש מסגרות פעולה שיאפשרו תגובה מהירה תוך שמירה על כללי החוק.
- **ביצוע הערכת סיכונים ייעודית** - לבחון אילו סוגי מידע עשויים להידרש, באילו תנאים, ולכמה זמן.
- **הטמעת מנגנוני מחיקה ובקרה** - להבטיח כי עם החזרה לשגרה תתבצע מחיקה של מידע עודף.
- **שקיפות ותקשורת עם הציבור** - להבהיר מראש ככל הניתן את מדיניות האיסוף והשימוש במידע.
- **חיזוק אבטחת הסייבר** - לוודא אמצעי הגנה מוגברים, לרבות הדרכת עובדים והיערכות מול מתקפות מתוחכמות.

לפרטים נוספים:

<https://www.gov.il/he/pages/lio080627>