שם המסמך : **תיק הגנת פרטיות ארגוני**	עמוד 1 מתוך 22
מספר הנוהל : **1**	תאריך תחולה : 1.1.2026
גרסה : **ראשונה**	תאריך עדכון : 1.1.2026

תיק הגנת הפרטיות – מסגרת ממשל פרטיות ארגונית

מועצה מקומית מג'ד אלכרום

להלן (״הארגון״)

מס'	אנשי קשר	פרטים	תאריך אישור
1	עורך	**רעות צבי ממונה הגנת פרטית**	1-1-2026
2	מאשר	**רבאח מנאע – מנכ״ל המועצה**	1-1-2026

שם המסמך : **תיק הגנת פרטיות ארגוני**	עמוד 2 מתוך 22
מספר הנוהל : **1**	תאריך תחולה : 1.1.2026
גרסה : **ראשונה**	תאריך עדכון : 1.1.2026

תוכן העניינים:

1. **מבוא ומטרות הנוהל** 3
2. **עקרונות לניהול מידע אישי** 3
3. **מסגרת חוקית ורגולטורית** 4
4. **הגדרות ותפקידים** 4
5. **מינויים וגורמי ממשל** 5
6. **אחריות** 6
7. **ועדת פרטיות ארגונית ואבטחת מידע** 7
8. **אחריות הדירקטוריון / הנהלת הארגון** 7
9. **ממונה הגנת הפרטיות(DPO)** 8
10. **השיטה** 9
11. **מחזור חיי המידע** 9
12. **ניהול מאגרי מידע** 12
13. **בסיס חוקי לאיסוף ועיבוד מידע** 12
14. **חובת יידוע ושקיפות** 13
15. **זכויות נושאי מידע** 13
16. **צמצום מידע ומניעת מידע עודף** 14
17. **שמירת מידע, ארכוב ומחיקה** 14
18. **העברת מידע לצדדים שלישיים** 15
19. **התקשרות עם ספקים (מעבדי מידע במיקור חוץ)** 15
20. **אבטחת מידע** 16
21. **בינה מלאכותית** 16
22. **תסקיר פרטיות לבינה מלאכותית** 17
23. **אירועי פרטיות ואבטחת מידע- תרשים זרימה** 17
24. **הדרכות והעלאת מודעות** 18
25. **בקרה, ביקורת ופיקוח רוחבי** 18
26. **פיקוח רוחבי מקיף** 18
27. **תיעוד ואחריותיות** 19
28. **אכיפה, סנקציות וקנסות** 19
29. **מדדי ביצוע בתחום הגנת הפרטיות** 19
30. **ניהול מסמכי פרטיות** 20
31. **תוכנית עבודה שנתית לפרטיות (Annual Privacy Plan)** 20
32. **מראי מקום** 21
33. **עדכון תיק הגנת הפרטיות** 22

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד : 072-250-4385 | email: office@iti-il.com

שם המסמך : **תיק הגנת פרטיות ארגוני**	עמוד 3 מתוך 22
מספר הנוהל : **1**	תאריך תחולה : 1.1.2026
גרסה : **ראשונה**	תאריך עדכון : 1.1.2026

1. מבוא ומטרות הנוהל

1.1 **מטרת הנוהל**

נוהל זה נועד להסדיר את עקרונות הגנת הפרטיות בארגון, לקבוע את קווי היסוד לפעילות עיבוד מידע אישי, להגדיר תפקידים וסמכויות, ולהבטיח עמידה מלאה בדרישות החוק ותקנותיו. הנוהל מהווה את ה"חוקה הארגונית" להגנה על זכויותיהם של נושאי המידע (עובדים, לקוחות, ספקים וצדדים שלישיים).

1.2 **תחולה**

הנוהל חל באופן רוחבי על כלל אגפי ומחלקות הארגון, על כל עובד, מנהל, קבלן משנה, ספק או נותן שירותים שיש לו גישה למידע אישי המנוהל בארגון או המעובד מטעמו.

1.3 **מטרות ההגנה על הפרטיות**

- שמירה על כבודם וזכותם החוקתית לפרטיות של כלל האנשים שמידע אודותיהם מעובד בארגון.
- הבטחת סודיות, שלמות וזמינות המידע האישי ומניעת גישה בלתי מורשית או זליגת נתונים.
- יצירת אמון מול הציבור, הלקוחות והעובדים כארגון השומר על ערכי הפרטיות.

1.4 **עקרון האחריותיות**

הארגון מאמץ את עקרון האחריותיות כעקרון על מוביל:

- **פרטיות היא אחריות ארגונית :** הגנת הפרטיות אינה משימה טכנולוגית בלבד של מחלקת המחשוב, אלא אחריות ניהולית ועסקית של כל מנהל אגף ומחלקה בארגון.
- **חובת עמידה בהוראות הדין :** על הארגון להוכיח באופן אקטיבי כי הוא פועל בהתאם להוראות החוק.
- **חובת תיעוד ובקרה :** פעולות שלא תועדו, לא הוכחו. הארגון יקיים מנגנון תיעוד שוטף של כל החלטות הפרטיות, סקרי הסיכונים והאישורים הניתנים.

2. עקרונות לניהול מידע אישי

הארגון יפעל בכל פעילות של איסוף, עיבוד, שימוש ושמירת מידע אישי בהתאם לעקרונות הבאים:

- עיבוד מידע למטרה חוקית, מוגדרת ומתועדת.
- איסוף המידע המינימלי הנדרש (צמצום מידע)
- שימוש במידע בהתאם למטרות שלשמן נאסף.
- שמירה על איכות, שלמות ועדכניות המידע.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד : 072-250-4385 | email: office@iti-il.com

- הגבלת תקופת שמירת המידע.
- יישום אמצעי אבטחת מידע מתאימים לאורך כל מחזור חיי המידע.
- שמירה על שקיפות כלפי נושאי המידע.
- תיעוד, בקרה ואחריותיות (Accountability) בכל שלבי עיבוד המידע.

3. מסגרת חוקית ורגולטורית

מדיניות זו מבוססת על המסגרת הנורמטיבית הבאה ועמידה בה היא חובה חקוקה:

- **חוק הגנת הפרטיות, התשמ"א-1981** ובמיוחד הוראות **תיקון 13, התשפ"ד-2024** שהרחיב משמעותית את חובות השקיפות, עקרון המידתיות וסמכויות האכיפה של הרשות.
- **תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017** להלן : "תקנות אבטחת מידע"
- **תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע מחוץ לגבולות המדינה), התשס"א-2001)** העברת מידע לחו"ל.
- **הנחיות ומדריכי הרשות להגנת הפרטיות** לרבות מדריך תסקיר השפעה על הפרטיות הנחיות בנושא מצלמות אבטחה, ושימוש בבינה מלאכותית.
- **חוק יסוד: כבוד האדם וחירותו** (סעיף 7 - הזכות לפרטיות).
- **חוקים ייעודיים החלים על הארגון** (כגון חוקי עבודה, חוק הארכיונים, חוקים פיננסיים או רגולציות מגזריות בהתאם לאופי הארגון).

4. הגדרות ותפקידים

4.1 **בעל השליטה במידע -** הארגון כישות משפטית המחליטה על מטרות עיבוד המידע ואופן הטיפול בו.

4.2 **מנהל מאגר מידע** - בעל השליטה, ולעניין גוף ציבורי סעיף 23-מנהל הכללי של הגוף או מי שהסמיכו לנהל (למשל : מנכ"ל, מנהל משאבי אנוש הוא מנהל מאגר עובדים). מנהל המאגר הוא הגורם העסקי האחראי על המידע בפועל.

4.3 **מחזיק מאגר / מעבד מידע -** גורם חיצוני המעבד את המידע עבור הארגון ומטעמו (לדוגמה : חברת ענן, מערכת שכר חיצונית).

4.4 **עיבוד מידע-** כול פעולה במידע (קבלתו, איסופו, עיון בו, חשיפתו, העברתו ,מסירתו או מתן גישה אליו.

4.5 **מידע אישי-**נתון הנוגע לאגם מזוהה או אדם הניתן לזיהוי במאמץ סביר בעקיפין או במישרין.

4.6 **מידע בעל רגישות מיוחדת-** מידע אישי על צנעת חיי משפחה, ביומטרי, מוצאו של אדם, עברו פלילי, דעותיו הפוליטיות או אמונתו, הערכת אישיות, נתוני מיקום ונתוני תעבורה, מידע על שכרו, חלה חובת סודיות, מצב בריאותו.

4.7 **ממונה הגנת הפרטיות -** גורם מקצועי מוגדר בארגון האחראי על הפיקוח, ייעוץ להנהלה ולעובדים, בחינת השפעה על הפרטיות, מענה לפניות הציבור וקידום הציות לדין.

4.8 **ממונה אבטחת מידע -** גורם מקצועי האחראי על יישום בקרות הגנת הסייבר, אבטחת התשתיות, השרתים, הרשאות הגישה הטכנולוגיות וטיפול טכני באירועי אבטחה.

4.9 **בעלי הרשאות -** עובדים או ספקים שהורשו לגשת למידע לצורך ביצוע תפקידם בלבד.

4.10 מנכ"ל והנהלה בכירה

4.11 **קווי דיווח ושיתוף פעולה**

- **מניעת ניגוד עניינים :** ממונה הגנת הפרטיות לא ימלא תפקיד המעמיד אותו בניגוד עניינים עם סמכויות הפיקוח שלו (כגון מנהל מערכות מידע או מנהל מאגר פעיל). ה **DPO-**ידווח ישירות למנכ"ל הארגון.
- **חובת שיתוף פעולה :** כל עובד ומנהל בארגון מחויב לשתף פעולה באופן מלא עם ה **DPO** וה **CISO-**לצורך יישום הוראות נוהל זה.

5. מינויים וגורמי ממשל

5.1 **כתבי מינוי רשמיים**

לא יופעל מאגר מידע בארגון ללא הגדרה חתומה בכתב של בעלי התפקידים הבאים:

- **כתב מינוי ממונה פרטיות :(DPO)** חובה בכל גוף ציבורי ובכל ארגון המעבד מידע רגיש בהיקף נרחב בהתאם לתיקון 13.(סעיף 8א)
- **כתב מינוי ממונה אבטחת מידע :(CISO)** ימונה על ידי הנהלת הארגון ויהיה בעל הכשרה מתאימה, חובה בגופים ציבורים סעיף 23 ,מעל 5 מאגרים החייבים ברישום, בנק חברת ביטוח הערכת אשראי.(סעיף 17ב)
- **כתבי מינוי מנהלי מאגרים** : לכל מאגר מידע בארגון ימונה מנהל מאגר בכתב, אשר יהיה אחראי לניהול המאגר בהתאם להוראות הדין ולנהלי הארגון. המינוי יתועד במסמך הגדרות המאגר ובתיק הגנת הפרטיות. מנהל המאגר יחתום על כתב מינוי, הצהרת סודיות והצהרת אחריות. במאגר מידע הטעון רישום, פרטי מנהל המאגר יעודכנו במסגרת בקשת הרישום או הודעת העדכון לרשות להגנת הפרטיות, בהתאם להוראות הדין.
- **כתב מינוי העברת מידע בין גופים ציבוריים**- יגדיר את הסמכות, האחריות והיקף ההרשאות לביצוע, אישור ובקרה על העברות מידע בין גופים ציבורים סעיף 23, בהתאם להוראות הדין ולנהלי הארגון.

- **כתב מינוי ועדת פרטיות וסייבר:** יגדיר את הרכב הוועדה, סמכויותיה ואחריותה לפיקוח, קבלת החלטות ומעקב אחר נושאי הגנת הפרטיות, אבטחת מידע, ניהול סיכונים ואירועי סייבר בארגון.

6. אחריות

6.1 האחריות ליישום תיק הגנת הפרטיות, לעדכונו, לבקרה על יישומו ולווידוא עמידת הארגון בדרישות חוק הגנת הפרטיות, התשמ"א-1981, תקנות הגנת הפרטיות (אבטחת מידע), תיקון 13, הנחיות הרשות להגנת הפרטיות והוראות כל דין, מוטלת על הנהלת הארגון, כאשר כל בעל תפקיד אחראי בתחום אחריותו.

6.2 להלן חלוקת האחריות בין בעלי התפקידים:

בעל תפקיד	תחום אחריות
מנכ"ל / הנהלת הארגון/דריקטוריון	**אחריות כוללת לעמידת הארגון בדרישות הדין, הקצאת משאבים, אישור מדיניות ותיק הגנת הפרטיות**
ממונה הגנת הפרטיות (DPO)	**פיקוח על יישום הוראות חוק הגנת הפרטיות, ליווי עמידה בדרישות הרגולציה, מתן ייעוץ מקצועי, בחינת תהליכי עיבוד מידע, ליווי תסקירי פרטיות, טיפול במימוש זכויות נושאי מידע, בחינת אירועי פרטיות והמלצה על חובת דיווח לרשות להגנת הפרטיות**
ממונה אבטחת המידע (CISO)	**יישום ובקרה של אמצעי אבטחת המידע, ניהול סיכוני סייבר, ניהול הרשאות, טיפול באירועי אבטחת מידע, בקרה על עמידה בתקנות אבטחת מידע והובלת ההיבטים הטכנולוגיים של אירועי פרטיות**
מנהל מערכות מידע (מנמ"ר)	**אחריות על התשתיות הטכנולוגיות, מערכות המידע, שרתים, גיבויים, מחיקות, תחזוקת המערכות ויישום דרישות אבטחת המידע במערכות הארגון**
היועץ המשפטי	**מתן חוות דעת משפטיות, בחינת בסיסים חוקיים לעיבוד מידע, ליווי הסכמי עיבוד מידע, מסירת מידע לגורמים חיצוניים וליווי הליכים מול רשויות**
מנהלי מאגרי המידע	**אחריות לניהול המאגרים שבתחום אחריותם, הגדרת מטרות המאגר, בחינת הצורך במידע, צמצום מידע, בקרת הרשאות, שמירת איכות המידע ועמידה בהוראות תיק הגנת הפרטיות**
כלל עובדי הארגון ובעלי ההרשאות	**יישום ההנחיות בתחום אחריותם, שמירה על סודיות המידע, דיווח מיידי על אירועי פרטיות או אבטחת מידע ושיתוף פעולה עם הגורמים המטפלים**

7. ועדת פרטיות ארגונית ואבטחת מידע

7.1 לצורך פיקוח, בקרה וקבלת החלטות בנושאי פרטיות, הוועדה תכלול, לפי העניין:

א. מנכ"ל
ב. ממונה הגנת הפרטיות(DPO)
ג. ממונה אבטחת המידע(CISO)
ד. מנמ"ר/מנהל מערכות מידע
ה. היועץ המשפטי
ו. מנהלי מאגרים ובעלי תפקידים נוספים לפי הצורך.

7.2 הוועדה תתכנס לפחות אחת לשנה, ובנוסף בעת הצורך, לצורך :
7.2.1 סקירת אירועי פרטיות.
7.2.2 סקירת תוכנית העבודה השנתית ומדדי הביצוע
7.2.3 בחינת סיכונים.
7.2.4 אישור פרויקטים חדשים.
7.2.5 בחינת תסקירי פרטיות.(DPIA)
7.2.6 סקירת תוכנית העבודה השנתית.
7.2.7 מעקב אחר ממצאי ביקורת.
7.2.8 בחינת שינויים רגולטוריים והשלכותיהם על פעילות הארגון.
7.2.9 קבלת החלטות בנושאי פרטיות.

הערה :אם בארגון אין ועדה ייעודית, ניתן להגדיר כי תפקידיה יבוצעו במסגרת ועדת ההיגוי לאבטחת מידע או הנהלת הארגון.

8. אחריות הדירקטוריון / הנהלת הארגון

8.1 לקבוע את מדיניות הארגון בתחום הגנת הפרטיות ואבטחת המידע ולאשרה.
8.2 לוודא קיומם של מנגנוני ממשל תאגידי לניהול סיכוני פרטיות וסייבר.
8.3 למנות את בעלי התפקידים הנדרשים (ממונה הגנת פרטיות, ממונה אבטחת מידע, מנהלי מאגרים, ועדת פרטיות וסייבר וכד)
8.4 להקצות משאבים מתאימים ליישום דרישות הדין, לניהול סיכונים ולהטמעת בקרות.
8.5 לקבל דיווחים תקופתיים על סיכוני פרטיות, אירועי אבטחת מידע, עמידה בדרישות הדין ותוכנית העבודה השנתית.
8.6 לפקח על יישום החלטות ולוודא טיפול בליקויים ובממצאי ביקורות.
8.6.1 אחריות ועדת פרטיות וסייבר
8.6.2 לסייע להנהלה בפיקוח על יישום הוראות חוק הגנת הפרטיות ותקנות אבטחת המידע.
8.6.3 לדון בסיכוני פרטיות, סיכוני סייבר וממצאי סקרי סיכונים ומבדקי חדירה.

8.6.4 לעקוב אחר יישום תוכניות העבודה בתחום הפרטיות ואבטחת המידע.

8.6.5 לדון באירועי אבטחת מידע משמעותיים, בהפקת לקחים ובאמצעי המניעה.

8.6.6 לבחון ולאשר עקרונית תהליכי עיבוד מידע חדשים, העברות מידע בין גופים, ושינויים מהותיים במאגרי מידע, בהתאם לנהלי הארגון.

8.6.7 לעקוב אחר יישום המלצות ביקורת פנימית, ביקורת חיצונית והרשות להגנת הפרטיות.

8.6.8 לקבל דיווחים תקופתיים מממונה הגנת הפרטיות, מממונה אבטחת המידע ומנהלי המאגרים.

8.6.9 להמליץ להנהלה על עדכון נהלים, הקצאת משאבים ופעולות לשיפור רמת הציות והבשלות הארגונית.

9. ממונה הגנת הפרטיות (DPO)

9.1 הארגון ימנה ממונה הגנת פרטיות (DPO), בהתאם להוראות הדין ובמקרים שבהם קיימת חובה לכך או בהתאם להחלטת הארגון.

9.2 ממונה הגנת הפרטיות יהיה גורם מקצועי עצמאי בתחום הגנת הפרטיות, ותפקידו לייעץ, להנחות, לפקח וללוות את הארגון ביישום הוראות הדין.

9.3 תחומי אחריותו של ממונה הגנת הפרטיות יכללו, בין היתר:

9.4 ייעוץ להנהלת הארגון ולבעלי התפקידים בכל הנוגע ליישום הוראות חוק הגנת הפרטיות, התקנות והנחיות הרשות להגנת הפרטיות.

9.5 פיקוח על עמידת הארגון בדרישות הדין, נהלי הארגון ותיק הגנת הפרטיות.

9.6 ליווי תהליכי עיבוד מידע חדשים, הקמת מאגרי מידע, שינויים מהותיים במאגרים והעברות מידע.

9.7 ליווי ובחינת תסקירי השפעה על הפרטיות (DPIA) וחוות דעת מקדמיות, בהתאם לצורך.

9.8 קידום מודעות ארגונית, הדרכות והטמעת תרבות של הגנת הפרטיות בקרב העובדים.

9.9 ליווי הטיפול באירועי פרטיות, בחינת השלכותיהם, המלצה על פעולות מתקנות ומעקב אחר יישומן.

9.10 קבלת פניות של נושאי מידע וליווי מימוש זכויותיהם בהתאם להוראות הדין.

9.11 מעקב אחר שינויים בחקיקה, בפסיקה ובהנחיות הרשות להגנת הפרטיות, והמלצה על התאמות נדרשות בארגון.

9.12 דיווח להנהלת הארגון ולוועדת הפרטיות ואבטחת המידע על מצב הציות, סיכונים, ליקויים והמלצות לשיפור.

9.13 עבודה שוטפת מול ממונה אבטחת המידע, מנהלי מאגרי המידע, היועץ המשפטי ובעלי תפקידים נוספים לצורך יישום דרישות הגנת הפרטיות בארגון.

שם המסמך : **תיק הגנת פרטיות ארגוני**	עמוד 9 מתוך 22
מספר הנוהל : **1**	תאריך תחולה : 1.1.2026
גרסה : **ראשונה**	תאריך עדכון : 1.1.2026

10. השיטה

11. מחזור חיי המידע

11.1 **מטרה**

11.1.1 הארגון ינהל את המידע האישי לאורך כל מחזור חייו, החל ממועד איסופו ועד למחיקתו או לארכובו, באופן המבטיח עמידה בהוראות חוק הגנת הפרטיות, תקנות הגנת הפרטיות (אבטחת מידע), עקרונות האחריותיות (Accountability), צמצום המידע (Data Minimization) שמירת מידע ואבטחתו.

11.1.2 ניהול מחזור חיי המידע נועד להבטיח כי בכל שלב של עיבוד המידע יבוצעו הבקרות הנדרשות, יוגדרו בעלי האחריות, ויישומו אמצעי הגנה מתאימים בהתאם לרמת הרגישות של המידע.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד : 072-250-4385 | email: office@iti-il.com

11.2 **עקרונות מחזור חיי המידע**

11.2.1 האיסוף, השימוש, השמירה, ההעברה והמחיקה של מידע אישי יתבצעו בהתאם לעקרונות הבאים :

11.2.1.1 עיבוד מידע יבוצע למטרה חוקית, מוגדרת ומתועדת.

11.2.1.2 ייאסף אך ורק המידע הנדרש להשגת מטרת המאגר.

11.2.1.3 השימוש במידע יוגבל למורשי גישה ובהתאם להרשאות שנקבעו.

11.2.1.4 מידע יישמר באופן מאובטח לאורך כל תקופת החזקתו.

11.2.1.5 מידע יועבר לגורמים פנימיים או חיצוניים רק בהתאם לדין, לעקרון צמצום המידע ובהתאם להרשאות המתאימות.

11.2.1.6 מידע שתמה תקופת השמירה שלו יימחק, יושמד או יעבור אנונימיזציה בהתאם למדיניות שמירת המידע של הארגון ולהוראות הדין.

11.3 **אחריות בעלי התפקידים לאורך מחזור חיי המידע**

בעל תפקיד	אחריות עיקרית
הנהלת הארגון	אישור מדיניות ומשאבים
מנהל המאגר	ניהול המידע לאורך כל מחזור חייו, קביעת מטרות, צמצום מידע, בקרות תקופתיות
ממונה הגנת הפרטיות (DPO)	פיקוח על עמידה בדין, ליווי מקצועי, בחינת חוקיות העיבוד ובקרת פרטיות
ממונה אבטחת המידע (CISO)	אבטחת המידע, ניהול סיכונים, בקרות אבטחה וטיפול באירועי אבטחה
מנמ"ר	תפעול המערכות, גיבויים, מחיקות, זמינות ותשתיות
היועץ המשפטי	בחינת בסיסים חוקיים, הסכמים והעברות מידע
כלל העובדים	שימוש במידע בהתאם להרשאות, שמירה על סודיות ודיווח על אירועי פרטיות

11.4 **שלבי מחזור המידע האישי-עקרונות מנחים**

11.4.1 מחזור חיי המידע מהווה מסגרת ניהולית לניהול מידע אישי בארגון לאורך כל תקופת עיבודו. בכל אחד משלבי המחזור נדרש לוודא כי עיבוד המידע מתבצע בהתאם למטרות המאגר, לבסיס החוקי, לעקרונות צמצום המידע, אבטחת המידע והגנת הפרטיות, תוך בחינה שוטפת של הסיכונים, תיעודם ויישום בקרות מתאימות בהתאם לשינויים בתהליכי העבודה, במערכות המידע ובדרישות הדין.

11.4.2 **הארגון יבחן באופן שוטף את תהליכי עיבוד המידע, הסיכונים, הבקרות והנהלים, ויעדכנם בהתאם לשינויים טכנולוגיים, רגולטוריים, ארגוניים ולממצאי ביקורות ואירועי פרטיות.**

שם המסמך : **תיק הגנת פרטיות ארגוני**	עמוד 11 מתוך 22
מספר הנוהל : **1**	תאריך תחולה : 1.1.2026
גרסה : **ראשונה**	תאריך עדכון : 1.1.2026

השלבים המפורטים לעיל מהווים מסגרת ניהולית בלבד. ההוראות התפעוליות לכל שלב מפורטות בנהלי הארגון הרלוונטיים

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד : 072-250-4385 | email: office@iti-il.com

שם המסמך: **תיק הגנת פרטיות ארגוני**	עמוד 12 מתוך 22
מספר הנוהל: **1**	תאריך תחולה: 1.1.2026
גרסה: **ראשונה**	תאריך עדכון: 1.1.2026

12. ניהול מאגרי מידע

12.1 **הקמת מאגר מידע**

הקמת מאגר מידע חדש בארגון או ביצוע שינוי מהותי במאגר קיים מחייבים וקבלת אישור הגורמים המוסמכים בארגון, ובכלל זה ה DPO-וה ,CISO-בהתאם לרמת הסיכון ולאופי המאגר.

12.2 **מסמך הגדרות מאגר (חובה חקוקה - תקנה 2)**

12.2.1 לכל מאגר מידע בארגון ינוהל מסמך הגדרות מאגר מעודכן שיאושר אחת לשנה ויכלול:

- מטרות המאגר המדויקות והבסיס החוקי לקיומו.
- סוגי המידע האישי שנשמרים בו (בדגש על סיווג מידע רגיש).
- מקורות המידע (ממי נאסף המידע).
- מקבלי המידע (צדדים שלישיים להם מועבר המידע).
- מורשי הגישה למאגר ורמות ההרשאה שלהם.
- זמני שמירת המידע המאושרים.
- המערכות התומכות והטכנולוגיות המשמשות לעיבוד המאגר.
- פירוט האם המאגר מועבר לחו"ל או מוחזק בענן חיצוני.

12.2.2 מסמך הגדרות המאגר ייבחן ויעודכן לפחות אחת לשנה או בעקבות שינוי מהותי במטרות המאגר, במידע המעובד, במערכות התומכות או בבסיס החוקי לעיבוד.

13. בסיס חוקי לאיסוף ועיבוד מידע

13.1 **הקמת מאגר מידע**

13.1.1.1.1 אין לאסוף או לעבד מידע אישי ללא קביעת בסיס חוקי מוגדר ומתועד מראש:

13.1.1.1.2 חובה חוקית / סמכות מכוח דין: עיבוד המידע נדרש לצורך עמידה בחובה חוקית המוטלת על הארגון (למשל: דיווח לרשויות המס, שמירת נתוני עובדים לפי חוקי עבודה).

13.1.1.1.3 ביצוע תפקיד ציבורי / אינטרס ציבורי: רלוונטי במיוחד לגופים ציבוריים ורשויות מקומיות הפועלים מכוח חוקי עזר ותקנות.

13.1.1.1.4 הסכמה מדעת: הסכמתו החופשית, המפורשת והמיודעת של נושא המידע.

13.1.1.1.5 אינטרס לגיטימי: הגנה על אינטרסים חיוניים של הארגון (כגון מניעת הונאות, אבטחת מידע וסייבר), ובלבד שאינטרס זה אינו פוגע באופן בלתי מידתי בזכויות ויסודות הפרטיות של הפרטי.

14. חובת יידוע ושקיפות

14.1 **הקמת מאגר מידע**

בעת פנייה לאדם לקבלת מידע אישי אודותיו, חובה להציג בפניו **הודעת פרטיות** נגישה, ברורה ובשפה פשוטה. ההודעה תוצג בנקודת האיסוף (טופס דיגיטלי, אתר אינטרנט, שיחת מוקד טלפוני וכיוצ"ב).

רכיבי הודעת הפרטיות החשובים:

א. **זהות בעל המאגר** ופרטי הקשר של ממונה הגנת הפרטיות(DPO)

ב. **מטרת איסוף המידע** והשימוש המתוכנן בו.

ג. **חובת מסירה :**האם חלה על האדם חובה חוקית למסור את המידע, או שמסירתו תלויה ברצונו הטוב ובהסכמתו.

ד. **התוצאות המשפטיות** או האחרות של אי-מסירת המידע.

ה. **מקבלי המידע :**האם המידע יועבר לצדדים שלישיים ובאילו תנאים.

ו. **פירוט זכויות נושא המידע :**לרבות זכות העיון, התיקון והמחיקה.

15. זכויות נושאי מידע

15.1 **הקמת מאגר מידע**

הארגון מחויב לאפשר לנושאי המידע לממש את זכויותיהם החוקיות בצורה יעילה ומהירה :

זכות העיון (סעיף 13 לחוק)

- כל אדם זכאי לעיין במידע עליו המוחזק במאגרי המידע של הארגון.

- **אימות זהות קשיח:** לפני מסירת מידע כלשהו לעיון, באחריות מנהל המאגר לבצע הליך אימות זהות קשיח (כגון זיהוי דו-שלבי, בקשת תעודה מזהה או אמצעי טכנולוגי מאובטח אחר) כדי למנוע הנדסה חברתית ומסירת מידע לצד שלישי מתחזה.
- **זכות התיקון והמחיקה (סעיף 14 לחוק)**
- מצא אדם כי המידע עליו אינו נכון, אינו שלם, אינו ברור או אינו מעודכן, הוא רשאי לפנות לבעל המאגר בבקשה לתקן את המידע או למחוק מידע עודף שאינו נדרש עוד למטרות המאגר.
- **זמני טיפול ובקרה (לוחות זמנים)**
- מענה ראשוני לבקשת עיון או תיקון יינתן **בתוך 30 יום** ממועד קבלת הבקשה.
- במידה והבקשה נדחית (כולה או חלקה), תימסר לפונה הודעה מנומקת בכתב, תוך ציון זכותו לערער לבית משפט השלום בהתאם לחוק.
- כל פנייה, הליך האימות, תוצאות הטיפול והמענה יתועדו ביומן פניות פרטיות ייעודי המנוהל על ידי הDPO

15.2 הארגון יפרסם באתר האינטרנט ובאמצעי הפנייה המקובלים את אופן הגשת הבקשות למימוש זכויות נושאי מידע.

16. צמצום מידע ומניעת מידע עודף

16.1 עקרון המידתיות

הארגון יאסוף ויעבד אך ורק את המידע האישי המינימלי הנדרש להשגת המטרה הלגיטימית שהוגדרה מראש.

הנחיה אופרטיבית:

- איסור מוחלט על איסוף מידע "למקרה שצריך": אין לאסוף שדות מידע עודפים, נתונים ביומטריים, מיקומי GPS או נתונים רגישים אחרים ללא צורך עסקי-חוקי מוכח ומתועד.
- בחינת נחיצות תקופתית: אחת לשנה, מנהלי המאגרים בתיאום עם ה DPO-יבצעו סקירה של טפסים דיגיטליים, שאלוני קליטה ותהליכי רישום, ויסננו שדות מידע עודפים שאינם חיוניים עוד לפעילות הארגון, יש לתעד כול פעולה של בדיקה זאת.

17. שמירת מידע, ארכוב ומחיקה

17.1 **קביעת זמני שמירה**

לכל סוג מידע בארגון ייקבעו זמני שמירה מוגדרים במסמך מדיניות שמירת מידע ארגונית, שיאושר על ידי היועץ המשפטי והנהלת הארגון בהתאם לחוק הארכיונים ולדיני ההתיישנות הרלוונטיים.

17.2 **מחיקה תקופתית בפועל**

מידע שתמה תקופת השמירה המותרת שלו יימחק או יעבור תהליך אנונימיזציה מלא (הסרת כל פרט מזהה באופן בלתי הפיך) כך שלא ניתן יהיה לשחזרו עוד.

17.3 **התמודדות עם מחיקה מגיבויים**

מחיקת מידע אישי משרתים ומערכות ייצור פעילות תבוצע באופן מיידי. מידע המצוי בקובצי גיבוי (Backups)אשר מחיקתו הפיזית אינה אפשרית טכנולוגית באותו הרגע ללא פגיעה בשלמות הגיבוי כולו, יטופל באופן הבא:

המידע יסומן במערכות הייצור ובבסיס הנתונים המרכזי כ"מידע מחוק לוגית"

במידה ויבוצע שחזור של קובץ הגיבוי עקב תקלה, יופעל תסריט (Script) אוטומטי שיבצע טיהור (Purge)מחדש של הנתונים שסומנו כמחוקים לוגית, טרם עליית המערכת המשוחזרת לאוויר הייצור.

18. העברת מידע לצדדים שלישיים

18.1 כל העברה של מידע אישי לגורם חיצוני תתבצע רק בכפוף לבסיס חוקי מוגדר, צמצום המידע למינימום הנדרש, ותיעוד מלא של ההעברה ביומן העברות מידע הכולל: תאריך, זהות המקבל, מטרת ההעברה והבסיס החוקי.

18.2 **העברת מידע בין גופים ציבוריים (סעיף 23 לחוק)**

העברת מידע דרך קבע או באופן חד-פעמי בין גופים ציבוריים תתבצע אך ורק בכפוף להוראות סעיפים 23ב-23ג לחוק הגנת הפרטיות, ובאמצעות הטפסים הרשמיים המצורפים לנספחי הציות של משרד המשפטים (טופס 7א, 7ב וטופס ג).

18.3 **העברת מידע לחו"ל**

העברת מידע לשרתים או גורמים מחוץ לגבולות מדינת ישראל תתאפשר רק בהתאם לתנאים הקבועים בתקנות העברת מידע לחו"ל, ותוך וידוא כי המדינה המקבלת מבטיחה רמת הגנה על הפרטיות שאינה פחותה מהרמה הקבועה בדין הישראלי (או תחת מנגנון הסכמי מחייב מתאים).

19. התקשרות עם ספקים (מעבדי מידע במיקור חוץ)

כל התקשרות עם ספק שירותים חיצוני (כגון שירותי ענן, תוכנה כשירות SaaS, - מערכות שכר או חברות אבטחה) המקבל גישה למידע האישי של הארגון, מחייבת יישום בקרות קשיחות (תקנה 15 לתקנות אבטחת מידע).

19.1 **בחינת נאותות ספקים(Due Diligence)**

לפני ההתקשרות, ה CISO-וה DPO-יבצעו הערכת סיכוני אבטחה ופרטיות לספק, לרבות מילוי שאלון אבטחת מידע ובחינת הסמכות לתקנים בינלאומיים ISO 27001, ISO 27701, SOC2

19.2 **הסכמי עיבוד מידע ונספחי אבטחה**

כל חוזה עם ספק יכלול נספח הגנת פרטיות ואבטחת מידע מחייב המגדיר:

- מטרות עיבוד המידע המותרות בלבד (איסור שימוש עצמי של הספק במידע)
- סוגי המידע וקטגוריות נושאי המידע.

- איסור על העסקת קבלני משנה (Sub-processors) ללא אישור מראש ובכתב מהארגון.
- חובת הספק לדווח על כל אירוע אבטחת מידע או חשד לאירוע בתוך 24 שעות לכל היותר.
- חובת הספק למחוק או להחזיר את כל המידע לארגון עם סיום ההתקשרות, ולספק אישור בכתב על ביצוע ההשמדה הפיזית.

19.3 **זכות ביקורת אקטיבית**

הארגון או נציג מוסמך מטעמו יהיו רשאים לבצע ביקורת אבטחת מידע ופרטיות במשרדי הספק ובמתקניו הפיזיים והטכנולוגיים, לפחות אחת לשנה ובתיאום מראש. הספק מתחייב לשתף פעולה באופן מלא ולהעמיד לרשות המבקרים את כל המסמכים המעידים על עמידתו בהתחייבויות אלו.

20. אבטחת מידע

קיים קשר ישיר ובלתי מנותק בין פרטיות לאבטחת מידע. הגנת הפרטיות לא תיתכן ללא בקרות סייבר חזקות שימנעו פריצה ודלף מידע.

20.1 **בקרות אבטחה מרכזיות:**

- **הרשאות גישה :** הרשאות גישה למידע אישי יינתנו באופן מצומצם ביותר, בהתאם להרשאה המזערית הנדרשת לביצוע התפקיד, ויבוצע סקר הרשאות חצי-שנתי חתום על ידי מנהלי המאגרים וה.CISO
- **הזדהות חזקה :** גישה מרחוק למערכות הארגון או גישה למערכות המכילות מידע רגיש תותנה בהזדהות רב-גורמית.
- **ניהול לוגים וניטור:** מערכות המידע יתעדו באופן אוטומטי, מאובטח ובלתי ניתן לשינוי פעולות של צפייה, עדכון, ייצוא ומחיקה של מידע אישי רגיש, לצורך זיהוי חריגות ובקרה בדיעבד.
- **הצפנה:** מידע אישי רגיש יוצפן במעבר (In Transit) באמצעות פרוטוקולים מאובטחים (כגון TLS 1.3 ובמנוחה (At Rest) בשרתים ובמסדי הנתונים.
- **ניהול גיבויים :**ביצוע גיבויים תקופתיים מוצפנים, ובדיקת שחזור (Restore Tests) חצי-שנתית מתועדת לווידוא שלמות המידע והיכולת לשחזרו בעת חירום.

21. בינה מלאכותית

הטמעת כלי בינה מלאכותית ארגוניים חוללה מהפכה תפעולית, אך היא מייצרת סיכוני פרטיות קריטיים, בייחוד בכל הנוגע לאימון מודלים על בסיס מידע אישי.

21.1 **שימוש אסור ומניעה טכנולוגית אקטיבית**

שם המסמך : **תיק הגנת פרטיות ארגוני**	עמוד 17 מתוך 22
מספר הנוהל : **1**	תאריך תחולה : 1.1.2026
גרסה : **ראשונה**	תאריך עדכון : 1.1.2026

- **איסור הזנת מידע אישי :** חל איסור מוחלט על עובדים וספקים להזין מידע אישי, מידע רפואי, פיננסי, נתוני עובדים או מידע רגיש אחר לתוך כלי AI ציבוריים כגון ChatGPT, Claude, Gemini בגרסאותיהם החינמיות / הציבוריות
- **אכיפה טכנולוגית :** מחלקת מערכות המידע תפעיל מערכות סינון תכנים (Web Filtering) ומערכות למניעת זלף מידע (DLP) על מנת לחסום באופן אקטיבי ניסיונות הזנה של מידע רגיש או גישה לא מורשית לממשקי AI ציבוריים שאינם מאובטחים.

22. תסקיר פרטיות לבינה מלאכותית

הטמעת כלי AI פנימיים או פיתוח מודלים בארגון מחייבים ביצוע **תסקיר השפעה על הפרטיות (DPIA)** מקיף טרם תחילת הפרויקט, לבדיקת סיכונים כגון קבלת החלטות אוטומטית מפלה, פגיעה בזכות העיון והסבר מודלים.

23. אירועי פרטיות ואבטחת מידע- תרשים זרימה

הגדרת אירוע פרטיות

אירוע פרטיות הוא כל אירוע שבו נחשף מידע אישי לגורם בלתי מורשה, שונה ללא הרשאה, נמחק באופן זדוני או אבד. **הבהרה קריטית :** גם שליחת הודעת דוא"ל או קובץ המכילים מידע אישי או רגיש לאדם הלא נכון (טעות אנוש בנמען) מהווה אירוע פרטיות חוקי לכל דבר ועניין ומחייבת דיווח וטיפול מיידי לגורמים המוסמכים לכך.

18.1 **חובת הדיווח הרגולטורית**

- במקרה של אירוע אבטחה חמור (במאגרים החלים עליהם רמת אבטחה בינונית או גבוהה), חלה חובת דיווח מיידית לרשות להגנת הפרטיות, וכן לנושאי המידע עצמם במידה והרשות הורתה על כך או שקיים סיכון ממשי לפגיעה בהם.
- הדיווח לרשות יבוצע **במיידי** מרגע הגילוי הראשוני.

24. הדרכות והעלאת מודעות

הגורם האנושי הוא לעיתים קרובות החוליה החלשה בשרשרת הגנת הפרטיות. הארגון יפעל להכשרת עובדיו באופן שוטף :

- **הדרכות עובדים תקופתיות :** כל עובד המקבל גישה למערכות המידע יעבור הדרכת מודעות לפרטיות ואבטחת מידע לפחות פעם בשנה. ההדרכה תכלול מבחן הבנה קצר.
- **תיעוד השתתפות :** כלל ההדרכות, שמות המשתתפים ותוצאות המבחנים יתועדו ויישמרו בתיק ה-DPO לצרכי הוכחת ציות (Accountability) בפני הרגולטור.
- **מבדקי פישיינג :** מחלקת אבטחת המידע תבצע מבדקי דיג (Phishing Simulation) תקופתיים ללא התראה מראש, למדידת ערנות העובדים ושיפור החוסן הארגוני.

25. בקרה, ביקורת ופיקוח רוחבי

תוכנית בקרה שנתית לפרטיות

ממונה הגנת הפרטיות (DPO) יכין ויבצע תוכנית בקרה וביקורת פנימית שנתית, שממצאיה יוצגו להנהלת הארגון ולוועדת ההיגוי.

26. פיקוח רוחבי מקיף

הביקורת השנתית לא תתמקד רק בהיבטים טכנולוגיים אלא תבצע בחינה שיטתית ורוחבית של כלל תחומי הפרטיות בארגון :

- **בחינת מאגרים :** האם כל המאגרים רשומים ומסמכי ההגדרות שלהם מעודכנים.
- **בקרת ספקים :** בדיקת מדגמית של ספקים פעילים ועמידתם בנספחי ה-DPA.
- **סקרי הרשאות :** לוודא כי הרשאות הגישה בפועל תואמות את הגדרות התפקיד.
- **בקרת העברות מידע :** בדיקת יומני ההעברות לצדדים שלישיים ולחו"ל.
- **בדיקת מנגנוני יידוע :** בדיקת תקינות הודעות הפרטיות בטפסים ובאתרי האינטרנט.
- **בקרת מחיקה ושימור :** וידוא כי מנגנוני המחיקה האוטומטיים והלוגיים פועלים כנדרש.
- **ביקורת AI ומצלמות :** וידוא עמידה בהוראות המיוחדות לשימוש בכלי בינה מלאכותית ובמצלמות אבטחה.(CCTV)

27. תיעוד ואחריותיות

הארגון פועל לפי הכלל המשפטי-רגולטורי המוביל: **אם פעולה לא תועדה בכתב - מבחינת הרגולטור היא מעולם לא בוצע** באחריות ה DPO-וה CISO-לנהל ולשמור בתיק הגנת הפרטיות הארגוני את המסמכים והיומנים הבאים:

- תיעוד מפורט של כלל החלטות ועדת ההיגוי והחלטות ניהוליות הנוגעות לעיבוד מידע.
- דוחות תסקירי השפעה על הפרטיות (DPIA/PIA) שנערכו לפרויקטים ומערכות חדשות.
- תיעוד סקרי סיכוני אבטחה ופרטיות שבוצעו בארגון וממצאי בדיקות חדירות (Penetration Tests).
- יומן אירועי אבטחה ופרטיות הכולל את תחקור האירוע, הפקת הלקחים ואופן הטיפול.
- אישורי הדרכות חתומים של העובדים.

28. אכיפה, סנקציות וקנסות

הפרת הוראות נוהל זה מהווה הפרת משמעת חמורה ועלולה לגרור סנקציות פנימיות וחיצוניות:

- **אחריות עובדים ומנהלים:** עובד או מנהל שיפר את הוראות הנוהל (כגון מסירת מידע ללא אימות, הזנת מידע רגיש ל AI-ציבורי, או מתן הרשאות גישה לא מורשות) יהיה כפוף להליכים משמעתיים, השעיית הרשאות, ועד לפיטורין בכפוף לשימוע כדין.
- **סמכויות האכיפה המורחבות של הרשות תיקון 13:** תיקון 13 הרחיב משמעותית את סמכויות האכיפה של הרשות להגנת הפרטיות, לרבות הטלת עיצומים כספיים דרמטיים (קנסות מנהליים של מאות אלפי שקלים לכל הפרה), דרישות מחייבות לתיקון ליקויים בצו מנהלי, והשעיית פעילות של מאגרי מידע.
- **אחריות אזרחית ופלילית:** פגיעה בזדון בפרטיותו של אדם, מסירת מידע ללא סמכות או רשלנות רבתי באבטחת מידע, עלולות להוביל להגשת תביעות אזרחיות נגד הארגון ונושאי משרה בו (לרבות תביעות ייצוגיות), וכן להעמדה לדין פלילי במקרים חמורים.

29. מדדי ביצוע בתחום הגנת הפרטיות

לצורך בקרה ושיפור מתמיד ימדוד הארגון, בין היתר:

א. מספר אירועי פרטיות.
ב. מספר בקשות למימוש זכויות.
ג. זמני טיפול בפניות.
ד. מספר תסקירי פרטיות.(DPIA)
ה. מספר ספקים שנבדקו.
ו. שיעור העובדים שהשלימו הדרכות פרטיות.
ז. עמידה בתוכנית העבודה השנתית.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד: 072-250-4385 | email: office@iti-il.com

שם המסמך: **תיק הגנת פרטיות ארגוני**	עמוד 20 מתוך 22
מספר הנוהל: **1**	תאריך תחולה: 1.1.2026
גרסה: **ראשונה**	תאריך עדכון: 1.1.2026

ח. ביצוע ביקורות פרטיות ואבטחת מידע.

נתוני המדדים יוצגו להנהלת הארגון כחלק מהבקרה התקופתית.

30. ניהול מסמכי פרטיות

כדי לשמור על תיק פרטיות חי, דינמי ומעודכן:

- **ניהול גרסאות:** כל עדכון של נוהל זה או נהלי המשנה הנגזרים ממנו יתועד בטבלת בקרת הגרסאות בראש המסמך, תוך פירוט השינויים שבוצעו וזהות העורך.
- **אישורי הנהלה ויועמ"ש:** כל גרסה חדשה של הנוהל מחייבת אישור מקצועי של ה DPO-וה-CISO, אישור משפטי של היועץ המשפטי של הארגון, ואישור ניהולי סופי של מנכ"ל הארגון.
- **בקרת מסמכים מבוזרת:** מסמך הגדרות המאגרים ונספחי ה DPA-של הספקים יישמרו בתיקיה מאובטחת ייעודית, המנוהלת תחת הרשאות גישה קפדניות של ה DPO-בלבד.

31. תוכנית עבודה שנתית לפרטיות *(Annual Privacy Plan)*

ממונה הגנת הפרטיות (DPO) יגבש עד ל-31 בדצמבר של כל שנה תוכנית עבודה שנתית מפורטת לשנה העוקבת, אשר תכלול:

- **יעדי פרטיות שנתיים:** למשל: סיום רישום כל המאגרים, השלמת הסכמי DPA מול 100% מהספקים הקריטיים
- **משימות אופרטיביות מוגדרות בזמן:** מועדי ביצוע ביקורות פנימיות, מועדי הדרכות עובדים, ביצוע תרגילי דימוי אירוע אבטחה ודלף מידע.
- **אחראים לביצוע:** הגדרת אחריות ברורה לכל משימה, DPO, CISO מנהלי מאגרים, מנמ"ר, משאבי אנוש.
- **מדדי הצלחה (KPIs) כמותיים:** למשל: הגעה ל-95% מעבר מבחני הבנה של עובדים, זמן מענה ממוצע לבקשות עיון הנמוך מ-15 יום
- **דיווח תקופתי להנהלה ולדירקטוריון:** הצגת סטטוס ביצוע תוכנית העבודה וממצאי הבקרה לוועדת ההיגוי לפחות פעם בחצי שנה.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד: 072-250-4385 | email: office@iti-il.com

שם המסמך: **תיק הגנת פרטיות ארגוני**	עמוד 21 מתוך 22
מספר הנוהל: **1**	תאריך תחולה: 1.1.2026
גרסה: **ראשונה**	תאריך עדכון: 1.1.2026

32. מראי מקום

נספח: מראי מקום להנחיות הרשות להגנת פרטיות

כדי להבטיח את מוכנות הארגון לביקורת, להלן טבלת קישורים והפניות רשמיות ("מראי מקום") המקשרת בין סעיפי התיק לבין ההנחיות, המדריכים וגילויי הדעת הרשמיים של הרשות להגנת הפרטיות בישראל:

סימוכין רשמי של הרשות	מראה מקום והנחיית הרשות להגנת הפרטיות הרלוונטית	נושא	מס' סעיף בתיק
הנחיית רשם מאגרי המידע מס' 2/2011 - ממונה הגנת פרטיות	גילוי דעת בנושא חובת מינוי ממונה הגנת פרטיות והגדרת תפקידיו בגופים ציבוריים ופרטיים.	מינוי ממונה הגנת פרטיות (DPO)	**סעיף 4**
מדריך הרשות להגנת הפרטיות לכתיבת מסמך הגדרות מאגר	תקנה 2 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 והמדריך המפורט של הרשות ליישומה.	מסמך הגדרות מאגר מידע	**סעיף 5**
גילוי דעת בנושא חובת יידוע לפי סעיף 11 לחוק הגנת הפרטיות	גילוי דעת והנחיות הרשות בדבר אופן ניסוח הודעות פרטיות והשגת הסכמה חוקית מנושאי המידע.	חובת יידוע ושקיפות (סעיף 11)	**סעיף 7**
הנחיות הרשות להגנת הפרטיות בדבר מימוש זכות העיון במאגרי מידע	מדריך מעשי לנושאי מידע ולארגונים למימוש זכות העיון במידע אישי וזכות התיקון לפי סעיפים 13-14 לחוק.	זכויות נושאי מידע (עיון ותיקון)	**סעיף 8**
נייר עמדה בנושא צמצום מידע עודף במאגרי מידע	מסמך מדיניות והנחיות של הרשות לעניין צמצום נתונים (Data Minimization) ומניעת החזקת מידע עודף שאינו נדרש עוד.	צמצום מידע ומניעת מידע עודף	**סעיף 9**
מדריך הרשות להגנת הפרטיות בנושא מחיקה ואנונימיזציה של מידע	מדריך הרשות להגנת הפרטיות ליישום תקנה 10 לתקנות אבטחת מידע - מחיקת מידע וניהול נכון של קובצי גיבוי.	שמירת מידע ומחיקה (גיבויים)	**סעיף 10**
הנחיית הרשות להגנת הפרטיות בנושא שימוש במיקור חוץ (תקנה 15)	הנחיה מפורטת לעניין יישום תקנה 15 לתקנות אבטחת מידע - אחריות הארגון בבחירת ספק, עריכת הסכם DPA וביצוע בקרות.	התקשרות עם ספקים (מיקור חוץ)	**סעיף 12**
מסמך עקרונות הרשות להגנת הפרטיות בנושא בינה מלאכותית ופרטיות	גילוי דעת והנחיות הרשות לעניין שימוש בטכנולוגיות בינה מלאכותית יוצרת (Generative AI)בארגונים וניהול סיכוני הפרטיות הכרוכים בהן.	בינה מלאכותית (AI)	**סעיף 14**

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד: 072-250-4385 | email: office@iti-il.com

שם המסמך: **תיק הגנת פרטיות ארגוני**	עמוד 22 מתוך 22
מספר הנוהל: **1**	תאריך תחולה: 1.1.2026
גרסה: **ראשונה**	תאריך עדכון: 1.1.2026

מדריך הרשות לדיווח על אירוע אבטחה חמור	הנחיות הרשות בנושא זיהוי, התמודדות וחובת דיווח על אירוע אבטחה חמור לרשות להגנת הפרטיות לפי תקנה 11 לתקנות אבטחת מידע.	אירועי פרטיות ואבטחת מידע	**סעיף 15**
הנחיית רשם מאגרי המידע מס' 4/2012 - מצלמות אבטחה	הנחיית רשם מאגרי המידע מס' 4/2012 בנושא שימוש במצלמות אבטחה ומצלמות מעקב במרחב הציבורי ובמבני הארגון.	שימוש במצלמות אבטחה(CCTV)	**מצלמות**
מדריך הרשות להגנת הפרטיות לעריכת תסקיר השפעה על הפרטיות	מדריך עזר מתודולוגי מפורט של הרשות לעריכת תסקיר השפעה על הפרטיות (Privacy Impact Assessment)לפרויקטים חדשים.	תסקיר השפעה על הפרטיות	**DPIA**

33. עדכון תיק הגנת הפרטיות

תיק הגנת הפרטיות ייבחן ויעודכן **לפחות אחת לשנה**, לצורך בחינת התאמתו להוראות הדין, להנחיות הרשות להגנת הפרטיות ולמדיניות הארגון.

33.1 בנוסף לבחינה השנתית, יעודכן התיק לפי הצורך במקרה של:

33.1.1 שינוי בהוראות הדין או בתקנות.

33.1.2 פרסום הנחיות, גילויי דעת או מסמכי מדיניות חדשים של הרשות להגנת הפרטיות.

33.1.3 שינוי מהותי במבנה הארגון או בממשל הפרטיות הארגוני.

33.1.4 החלטת הנהלת הארגון או ממונה הגנת הפרטיות כי נדרש עדכון התיק.

33.1.5 האחריות המקצועית לבחינה ולעדכון תיק הגנת הפרטיות מוטלת על ממונה הגנת הפרטיות **(DPO)**בשיתוף **ממונה על אבטחת המידע** ,**(CISO)** היועץ המשפטי ובעלי תפקידים רלוונטיים, לפי הצורך.

33.2 כל גרסה מעודכנת של תיק הגנת הפרטיות תאושר על-ידי בעל השליטה במידע ,באמצעות מנכ"ל הארגון או הגורם המוסמך מטעמו, ותיכנס לתוקף ממועד אישורה.

33.3 כל עדכון יתועד בטבלת בקרת הגרסאות ויאושר בהתאם למנגנון אישור המסמכים של הארגון.

מסמך נערך על ידי חברת תשתיות מידע וטכנולוגיות בע"מ | משרד: 072-250-4385 | email: office@iti-il.com