

מסמך ד'

כתב התחייבות- הגנת פרטיות

התחייבות זו מהווה חלק בלתי נפרד מהסכם מס' _____ למתן שירותי ניהול ותפעול לניסוי נעים לירוק 3 ("ההסכם") בין חברת נתיבי איילון בע"מ (כהגדרתה בהסכם – "החברה") לבין _____ (כהגדרתו בהסכם – "המפעיל") ביום _____ אשר תנאיו חלים על יחסי הצדדים יחד עם תנאי התחייבות זו.

במסגרת ההתקשרות בין הצדדים, יספק המפעיל לחברה שירותי ניהול ותפעול של ניסוי, המפורטים בהסכם ובמפרט השירותים המצורף להסכם כנספח ו' (כהגדרתם בהסכם – "השירותים"). כחלק ממתן השירותים תהיה למפעיל גישה למידע אישי אודות המתנדבים (כהגדרתם בהסכם) לרבות נתונים אישיים של המתנדבים, המידע המתקבל ממכשירי הניטור המותקנים ברכבם, תוצאות הניסוי ונתוני ההתחשבות עם המתנדבים וכל מידע נוסף הנוגע למתנדבים ("המידע") אשר יישמר במאגר מידע שיוחזק על-ידי המפעיל (כהגדרתו בהסכם – "מאגר המידע"). לכן מתחייב המפעיל כדלקמן:

1. הודעה והסכמה. בהתאם להוראות חוק הגנת הפרטיות, תשמ"א-1981 ("החוק"), מתחייב המפעיל לקבל את הסכמת המתנדבים מראש ובכתב טרם איסוף כל מידע אודותם, לאיסוף המידע, לשימוש להחזקתו ועיבודו במאגר המידע למטרת ניהול ניסוי נעים לירוק 3 בלבד ("המטרה"), לרבות הסכמה למדיניות פרטיות שתאושר על ידי החברה. מבלי לגרוע משאר התחייבויות המפעיל, פניית המפעיל למתנדבים לקבלת הסכמה זו תיעשה באמצעות הודעה אשר תציין: א) שמסירת המידע תלויה בהסכמת המתנדב ואין חובה חוקית למסור המידע; ב) שמסירת המידע הינה לצורך המטרה; ו-ג) למי יימסר המידע ומטרות המסירה.

2. מטרת השימוש במידע. המפעיל מתחייב לעשות שימוש במידע אך ורק לצורך המטרה.

3. מתן זכות עיון ותיקון. המפעיל יעמוד בדרישות סעיפים 13 ו-14 לחוק, ויאפשר למתנדבים, לבאי כוחם או לאפוטרופוס שלהם לעיין במידע אודותם תוך 7 ימים מקבלת בקשת העיון, ולבקש לתקן או למחוק מידע זה ויעדכן את המתנדבים אודות זכויותיהם ודרכי מימושם.

4. אבטחת מידע. המפעיל יעמוד בדרישות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("תקנות האבטחה"), החלות על מאגרי מידע בעלי רמת אבטחה גבוהה כהגדרתם בתקנות האבטחה, היתר לרבות ומבלי לגרוע:

4.1 ממונה על אבטחה. המפעיל ימנה ממונה על אבטחת מידע ("הממונה") בהתאם לסעיף 17ב לחוק וסעיף 3 לתקנות האבטחה. הממונה יהיה כפוף ישירות למנהל מאגר המידע ויהיה אחראי, בין היתר, על הכנת נוהל האבטחה (כמפורט בסעיף 4.2 להלן) ותכנית לבקרה שוטפת על עמידת המפעיל בדרישות תקנות האבטחה. המפעיל יקצה לממונה את המשאבים הדרושים לשם מילוי תפקידו.

4.2 נוהל אבטחה. המפעיל ינסח נוהל אבטחה בהתאם למסמך הגדרות מאגר המידע, ובהתאם לראשי הפרקים המצורפים להתחייבות זו כנספח א' ותקנות האבטחה לרבות סעיפים 2 ו-4 לתקנות האבטחה. המפעיל ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לגורמים המורשים (כהגדרתם בסעיף 5.2 להלן) רק בהיקף נדרש לצורך ביצוע תפקידם. אחת לשנה, המפעיל יבחן את הצורך בעדכון נוהל האבטחה, אלא אם כן: א) נעשו שינויים מהותיים במערכות מאגר המידע או בתהליכי עיבוד המידע; או ב) נודע למפעיל על סיכונים טכנולוגיים חדשים הנוגעים למערכות מאגר המידע. במקרים אלה המפעיל יבחן באופן מיידי את הצורך בעדכון נוהל האבטחה.

- 4.3 מסמך מבנה מאגר המידע ורשימת מערכות מאגר המידע. המפעיל יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות מאגר המידע בהתאם לראשי הפרקים המצורפים להתחייבות זו **כנספח ב'** ותקנות האבטחה לרבות סעיף 5 לתקנות האבטחה. המפעיל ימסור את הפרטים הכלולים במסמכים הנ"ל אך ורק לעובדיו המורשים ורק בהיקף הנדרש לצורך ביצוע תפקידיהם.
- 4.4 סקר סיכונים. המפעיל יערוך, אחת ל-18 חודשים, סקר לאיתור סיכוני אבטחת מידע בהתאם לסעיף 5 לתקנות האבטחה, ידון בתוצאות הסקר, יבחן את הצורך בעדכון נוהל האבטחה ויתקן כל ליקוי שיתגלה במסגרת הסקר.
- 4.5 מבדקי חדירות. המפעיל יערוך, אחת ל-18 חודשים, מבדקי חדירות למערכות מאגר המידע לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, ידון בתוצאות מבדקי החדירות ויתקן כל ליקוי שיתגלה במסגרת מבדקי החדירות ויעמוד בתנאי סעיף 5 לתקנות האבטחה.
- 4.6 אבטחה פיזית וסביבתית. המפעיל ישמור את מערכות מאגר המידע בהתאם לסעיף 6 לתקנות האבטחה. מערכות מאגר המידע יישמרו במקום מוגן המונע חדירה וכניסה אל מאגר המידע בלא הרשאה, והתואם את אופי פעילות מאגר המידע ורגישות המידע. המפעיל יבקר ויתעד כל כניסה ויציאה מאתרים שבהם מצויות מערכות מאגר המידע וכל הכנסה והוצאה של ציוד אל מערכות מאגר המידע ומהן.
- 4.7 אבטחת מידע בניהול כוח אדם. המפעיל לא יאפשר גישה למידע ולא ישנה את היקף ההרשאה שניתן לגורם המורשה, אלא רק לאחר שנקט אמצעים סבירים, המותאמים לרגישות המידע ולהיקף הרשאת הגישה שניתן, כדי לוודא שהגורם המורשה מתאים לקבלת גישה למידע, ורק לאחר שקיים הדרכה לגורם המורשה בנושא חובותיו על-פי נוהל האבטחה והחוק. בכל מקרה, אחת לשנתיים יקיים המפעיל הדרכות לכלל הגורמים המורשים באשר לחובותיהם על-פי נוהל האבטחה, תקנות האבטחה והחוק, בהיקף הנדרש לצורך ביצוע תפקידיהם, ויעמוד המפעיל בתנאי סעיף 7 לתקנות האבטחה.
- 4.8 ניהול הרשאות גישה. המפעיל יקבע הרשאות גישה למידע ולמערכות מאגר המידע, בהתאם לתנאי סעיף 8 לתקנות האבטחה, להגדרות תפקיד ובמידה הנדרשת לביצוע התפקיד בלבד וינהל רשימה מעודכנת של תפקידים, הרשאות הגישה שניתנו לכל תפקיד והגורמים המורשים (**"רשימת ההרשאות התקפות"**).
- 4.9 זיהוי ואימות. המפעיל יעמוד בתנאי סעיף 9 לתקנות האבטחה וינקוט אמצעים מקובלים בהתאם לאופי מאגר המידע וטיבו כדי לוודא שהגישה למידע ולמערכות מאגר המידע נעשית בידי הגורמים המורשים לפי רשימת ההרשאות התקפות. כאשר גורם מורשה מסיים את תפקידו, המפעיל יבטל את הרשאתו וישנה מיידית את הסיסמאות למאגר המידע ולמערכותיו. כמו כן, המפעיל יודא כי אופן הזיהוי ייעשה על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של הגורם המורשה (למשל באמצעות תעודה המכילה חתימה אלקטרונית מאובטחת).
- 4.10 בקרה ותיעוד גישה. המפעיל ינהל מנגנון תיעוד אוטומטי, אשר נתוניו יישמרו במשך שנתיים, שיאפשר ביקורת על הגישה למערכות מאגר המידע (**"מנגנון הבקרה"**) ובכלל זה נתונים אלו: (א) זהות המשתמש; (ב) התאריך והשעה של ניסיון הגישה; (ג) רכיב המערכת שאליו בוצע ניסיון הגישה; (ד) סוג הגישה והיקפה; (ו-ה) אם הגישה אושרה או נדחתה. המפעיל ידאג שמנגנון הבקרה לא יאפשר ביטול או שינוי של הפעלתו ושיפיץ התראות לאחראים במידה ואירע שינוי או ביטול שכזה. כמו כן, המפעיל יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח

של הבעיות שהתגלו והצעדים שננקטו בעקבותיהן. המפעיל יידע את הגורמים המורשים בדבר קיום מנגנון הבקרה ויעמוד בתנאי סעיף 10 לתקנות האבטחה.

4.11 אירוע אבטחה. הפעיל יעמוד בתנאי סעיף 11 לתקנות האבטחה ויתעד, באמצעות מנגנון רישום אוטומטי, כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה ("אירוע אבטחה"), יודיע על אירוע האבטחה לחברה ולרשם מאגרי המידע וידווח לרשם אודות הצעדים שננקטו בעקבות אירוע האבטחה. רשם מאגרי המידע עשוי להורות למפעיל להודיע על אירוע האבטחה למתנדבים שנפגעו בעקבותיו. בנוסף, אחת לרבעון יקיים המפעיל דיון באירועי האבטחה שאירעו ויבחן את הצורך בעדכון נוהל האבטחה בעקבותיהם.

4.12 התקנים ניידים. המפעיל יעמוד בתנאי סעיף 12 לתקנות האבטחה ויגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות מאגר המידע בהתאם לרגישות המידע ולאמצעים הקיימים להגנה על המידע. כמו כן, המפעיל יאפשר חיבור התקנים ניידים או העתקת המידע להתקן הנייד תוך נקיטת אמצעי הגנה (לרבות הצפנה של המידע שהועתק להתקן הנייד) ובשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן הנייד.

4.13 ניהול מאובטח ומעודכן של מערכות מאגר המידע. המפעיל ינהל ויתפעל את מערכות מאגר המידע בהתאם לסעיף 13 לתקנות האבטחה ובאופן תקין לפי המקובל בהפעלת מערכות כאלה. בנוסף, המפעיל יפריד בין מערכות מאגר המידע לבין מערכות מחשוב אחרות המשמשות את המפעיל (לדוגמה באמצעות מערכת fire wall (חומת אש) פנימית, מערכת לחלוקת רשתות ועוד). כמו כן, המפעיל יערוך עדכונים שוטפים של מערכות מאגר המידע, ולא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

4.14 אבטחת תקשורת. המפעיל יעמוד בתנאי סעיף 14 לתקנות האבטחה יודא כי מערכות מאגר המידע לא יחוברו לרשת האינטרנט או לכל רשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב. המפעיל יעביר את המידע ברשת ציבורית או האינטרנט רק לאחר הצפנת המידע המועבר. במידה וניתן יהיה לגשת למאגר המידע מרחוק באמצעות רשת האינטרנט או רשת ציבורית אחרת, המפעיל יעשה שימוש גם באמצעי פיזי הנתון לשיטתו הבלעדית של הגורם המורשה, כגון כרטיס חכם.

4.15 ביקורות תקופתיות. אחת לשנתיים יערוך המפעיל ביקורת פנימית או חיצונית בהתאם לתנאי סעיף 16 לתקנות האבטחה, על-ידי גורם המוכשר לכך, לצורך ווידוא עמידת המפעיל בהוראות תקנות האבטחה. המפעיל ידון בדוחות הביקורת שיועברו אליו בתום הביקורת ויבחן את הצורך בעדכון נוהל האבטחה בעקבותיהם.

4.16 שמירת נתוני אבטחה. המפעיל יעמוד בתנאי סעיף 17 לתקנות האבטחה וישמור את מידע אודות ניהול הרשאות גישה (סעיף 4.8), זיהוי ואימות (סעיף 4.9), אירועי אבטחה (סעיף 4.11) ואבטחת תקשורת (סעיף 4.14) למשך שנתיים ויגבה נתונים אלו באופן שיבטיח שיהיה ניתן בכל עת לשחזר אותם למצבם המקורי.

4.17 גיבוי ושחזור. המפעיל יעמוד בתנאי סעיף 18 לתקנות האבטחה ויקבע במסמך: א) נהלים לביצוע גיבוי ואבטחת שחזור כמפורט בסעיף 4.16 לעיל; ו-ב) כי במסגרת תיעוד אירועי אבטחה על-פי האמור בסעיף 4.11 לעיל, יתועדו גם הליכי שחזור המידע ובכלל זה זהותו של מבצע הליכי השחזור ופרטי המידע ששוחזר. כמו כן, המפעיל ישמור את עותק הגיבוי של הנתונים כאמור

בסעיף 4.16 לעיל ושל הנהלים להבטחת שחזור נתונים אלה באופן שיבטיח את שלמות המידע ואת אפשרות השחזור במקרה של אבדן או הרס.

מיקור חוץ

.5

- 5.1 העברת מידע. המפעיל לא יעביר לצדדים שלישיים את המידע לכל מטרה אחרת שאינה המטרה.
- 5.2 גורמים מורשים. מבלי לגרוע מהאמור בסעיפים 4.7-4.9 לעיל, המפעיל ינקוט באמצעי הזהירות הנדרשים על-מנת לוודא שהגישה למידע ניתנת אך ורק לעובדים מורשים של המפעיל הצריכים גישה זו לצורך מימוש המטרה ("גורמים מורשים"). על המפעיל להבטיח כי השימוש במידע יהיה מידתי ולצורך המטרה בלבד. המפעיל ידריך את הגורמים המורשים במטרות השימוש במידע. שימוש במידע לכל מטרה אחרת יהווה הפרה יסודית של ההסכם ושל התחייבות זו. המפעיל לא יעביר מידע לצד ג' כלשהו לרבות קבלני משנה ללא אישור מראש ובכתב מהחברה.
- 5.3 סודיות. מבלי לגרוע מהתחייבות המפעיל לשמירה על סודיות המצורף כנספח ג' להסכם, המפעיל יודא שבטרם מתן גישה למידע, כל הגורמים המורשים יהיו חתומים על התחייבות לשמירה על סודיות שתעמוד בחובות הסודיות בסעיף 16 לחוק.
- 5.4 אכיפה ודיווח. המפעיל יודא שהוראות התחייבות זו יאכפו באופן שוטף ויעביר הדרכות ויעדכן את הגורמים המורשים אודות המטרה והשימוש במידע. בנוסף, המפעיל, על-פי בקשתה הסבירה של החברה, ידווח לחברה לגבי עמידתו באמצעי האבטחה, בהסכם ובהתחייבות זו.
- 5.5 תיעוד. המפעיל ישמור תיעוד לעניין ציות להוראות התחייבות זו, לרבות ומבלי לגרוע לגבי חקירות ובדיקות של תלונות או הפרות אפשריות של התחייבות זו. המפעיל יציג את התיעוד האמור בפני החברה לפי דרישה ו/או בפני הרשות להגנת הפרטיות כפי שנדרש על-פי החוק או התחייבות זו.
- 5.6 ביטוח. מבלי לגרוע מאחריות המפעיל על-פי ההסכם, התחייבות זו ו/או על-פי כל דין, המפעיל מתחייב, כי בכל משך תקופת ההסכם, יקיים, יערוך ויחזיק בידיו, על חשבונו ביטוחים כמפורט באישור עריכת ביטוח המצורף להסכם כנספח יג'.
- 5.7 שימוש לא חוקי. בשום אופן המפעיל לא יאסוף, יעבד או ישתמש במידע או במאגר המידע למטרות לא מורשות או לא חוקיות.
- 5.8 ביקורת אבטחה. החברה ו/או הרשות להגנת הפרטיות יהיו רשאיות לבצע ביקורות תקופתיות אצל המפעיל, על-מנת לוודא כי המפעיל מקפיד לקיים את הוראות ההסכם ואת ההנחיות והדרישות המפורטות בהתחייבות זו וכן את הוראות הדין החל, וזאת בתיאום מראש עם המפעיל.
- 5.9 ביקורת באתר. המפעיל יאפשר לחברה ו/או לרשות להגנת הפרטיות לבצע ביקורות, לרבות ביקורות פתע, באתרי המפעיל שבהם נעשה שימוש במידע. במסגרת ביקורות אלו המפעיל ייתן לחברה ו/או לרשות להגנת הפרטיות גישה לכל חומר מחשב, אמצעי אחסון אלקטרוני או מכשיר שבו המידע מאוחסן ו/או מעובד.
- 5.10 הפרדת מידע. במקרה שבו המפעיל מספק שירותים בקשר עם מאגרי מידע של צדדים שלישיים, המפעיל יודא שישנה הפרדה פיזית ו/או לוגית בין המידע לבין מידע של צדדיים שלישיים אלו. לבקשת החברה ובכפוף לאישור בכתב, המפעיל ימנה איש קשר אחראי על כל עניין שקשור לשימוש במידע ואבטחת המידע. לבקשת החברה, המפעיל ישמר הפרדה מבנית בתוך התאגיד שלו על-מנת לצמצם ככל הניתן סיכון לשימוש במידע לצרכיו האחרים.

5.11 שמירת המידע. המפעיל ימחק מרישומיו ומאגריו כל מידע או חלק ממנו שאינו נחוץ למטרה והכל בהתאם להוראות החברה. במקרה שבו יש דרישה על-פי חוק לשמור חלק מהמידע, אזי מידע זה יישמר בנפרד פיזית או לוגית, מכל מידע אחר, באופן שבו ימזער אפשרות לשימוש בלתי מורשה ותנאי התחייבות זו ימשיכו לחול לגבי מידע זה. עם מחיקה של המידע לאחר סיום או ביטול ההסכם, יספק המפעיל לחברה הצהרה חתומה על-ידי מורשה החתימה של המפעיל שמאשרת כי המידע נמחק.

5.12 מסמך אבטחת מידע מיקור חוץ. המפעיל יעמוד בדרישות מסמך אבטחת מידע מיקור חוץ של החברה, כאשר העתק של מסמך זה יהיה נגיש למפעיל מיד לאחר חתימת התחייבות זו, ויהווה חלק בלתי נפרד מהתחייבות זו. מסמך אבטחה זה יתייחס בין היתר לנושאים הבאים: א) אבטחה פיזית; ב) אבטחה לוגית; ג) הפרדה של המידע; ד) מדיניות לעניין סיום השימוש במידע והסרת ציוד אחסון המידע; ה) תהליכים שקשורים למיון המידע; ו) נגישות שליטה; ז) חובות סודיות של גורמים מורשים; ח) ביקורת; ט) גיוס עובדים ובדיקות רקע (בין היתר, בנוגע להכשרת עובדים בעניין חובות זהירות בהקשר למידע), ו-י) ציות להוראות אבטחה נוספות, כולל אלו הכלולים בת"י ISO 27001 או בתקן אחר שאינו פחות מחמיר.

6. המפעיל ישפה את החברה ומי מטעמה, כולל ומבלי לגרוע את כל בעליה, מנהליה, בעלי המשרה, הגורמים הקשורים אליה ועובדיה נגד כל אבדן, הוצאה, עלויות, תביעות, פיצויים (כולל הוצאות סבירות בשל שכר טרחת עו"ד, תעריפי מומחים וכל הוצאה סבירה אחרת הקשורה בהתדיינות משפטית), הנובעים מ ו/או שבאופן כלשהו קשורים לתנאי התחייבות זו.

7. המפעיל מצהיר כי הוא מודע לכך שהתחייבות זו הינה חלק בלתי נפרד מההסכם וכי כל הפרה של התחייבות זו תחשב כהפרה יסודית של ההסכם ותזכה את החברה בכל סעד על-פי דין.

8. המפעיל מצהיר כי הוא מודע לכך שבכל מקרה של הפרת התחייבות זו, ומבלי לגרוע מכל זכות וסעד העומדים לחברה לפי כל דין ו/או בהתאם להסכם או לכתב התחייבות זה, יחולו הוראות סעיף 7 בהסכם שלהלן לעניין פיצויים מוסכמים, בסכומים ובתנאים הקבועים בנספח יד' להסכם.

9. המפעיל מצהיר כי הוא מודע לכך שהפרת התחייבות זו עלולה לגרום לחברה נזקים חמורים ביותר ובלתי הפיכים אשר פיצוי כספי לא יהווה תרופה וסעד נאות להם, ולפיכך המפעיל מסכים כי החברה תהיה זכאית, במקרה של הפרת התחייבות זו, לבקש מבית משפט מוסמך להוציא נגדו צו מניעה זמני ו/או צווים אחרים במטרה למנוע ו/או להפסיק את ההפרה.

ולראיה על החתום:

[המפעיל]

על-ידי:

שם:

תפקיד:

תאריך:

נספח א' - נוהל האבטחה

1. האבטחה הפיזית והסביבתית [יש לפרט הוראות לעניין האבטחה הפיזית והסביבתית של אתרי מאגר המידע, שכן תקנות האבטחה דורשות שמערכות מאגר המידע יישמרו במקום מוגן המונע חדירה וכניסה בלא הרשאה]
2. הרשאות גישה למאגר המידע [יש ליצור רשימת הרשאות גישה ושרשימה זו תעודכן באופן שוטף. הרשאות הגישה צריכות להינתן לפי תפקיד. הרישום יכלול את התפקיד שלו ניתנת הרשאה, את סוג הרשאת הגישה שניתנה לתפקיד זה ואת הגורמים המורשים הממלאים תפקידים אלה]
3. אמצעים המגנים [יש לפרט את האמצעים המגנים על מערכות מאגר המידע ואופן הפעלתם לצורך כך]
4. הוראות הגנת מידע [יש פרט הוראות לכלל הגורמים המורשים בנוגע להגנה על המידע]
5. הסיכונים [יש לפרט: את הסיכונים שחשוף להם המידע במסגרת הפעילות השוטפת של המפעיל, לרבות אלה הנובעים ממבנה מערכות מאגר המידע (המפורט בנספח ב' להלן); אופן קביעת סיכונים אלה; ואופן הטיפול בהם, לרבות על-ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר המידע או במערכותיו]
6. אירועי אבטחת מידע [יש לפרט את אופן התמודדות המפעיל עם אירועי אבטחת מידע בהתאם לחומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות גישה וצעדים מידיים אחרים, וכן לעניין דיווח על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם]
7. התקנים ניידים [יש לפרט הוראות לעניין ניהול של ושימוש של התקנים ניידים (התקן נייד הינו כל מצא המשמש לאחסון חומר מחשב למשל מחשב נייד, disc on key וטלפון סלולארי חכם). יש להגביל/למנוע אפשרות לחיבור התקנים ניידים למערכות מאגר המידע, וזאת ייקבע בהתאם לרגישות המידע, לסיכונים המיוחדים למערכות מאגר המידע/למידע הנובעים מחיבור ההתקן הנייד ולקיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד]
8. זיהוי ואימות [יש לפרט את אמצעי הזיהוי והאימות לגישה למאגר המידע ולמערכותיו בהתאם לאמור בסעיף 4.9 להתחייבות זו. במידה ואופן הזיהוי מבוסס על סיסמאות, על המפעיל להתייחס לחוזק הסיסמה, מספר הניסיונות השגויים ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד הגורם המורשה ובכל מקרה לתקופה שלא תעלה על שישה חודשים. בנוסף, על המפעיל להתייחס לניתוק אוטומטי של הגורם המורשה לאחר פרק זמן של אי פעילות אותו יש להגדיר כאן. כמו כן, יש להתייחס כאן לאופן הטיפול בתקלות הקשורות באימות זהות]
9. הבקרה על שימוש [יש לפרט את אופן הבקרה על שימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות מאגר המידע בהתאם לאמור בסעיף 4.10 להתחייבות זו]
10. ביקורות תקופתיות [יש לפרט הוראות לעניין עריכת ביקורת תקופתית לוודא קיומם ותקינותם של אמצעי האבטחה בהתאם לאמור בסעיף 4.15 להתחייבות זו]
11. גיבוי נתונים [יש לפרט הוראות לעניין גיבוי נתונים בהתאם לאמור בסעיף 4.17 להתחייבות זו]
12. פעולות פיתוח [יש פרט הוראות לעניין אופן ביצוע פעולות פיתוח ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר המידע]

נספח ב' - רשימת מצאי של מערכות מאגר המידע

1. תשתיות ומערכות חומרה במאגר המידע [יש לכלול את סוגי רכיבי תקשורת ואבטחת מידע]
2. מערכות התוכנה במאגר המידע [יש לפרט מערכות המשמשות להפעלת מאגר המידע, לניהול, לתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו]
3. תוכנות וממשקים [יש לפרט את התוכנות והממשקים המשמשים לתקשורת אל מערכות מאגר המידע]
4. תרשים הרשת שמאגר המידע פועל בו [יש לכלול את תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה].

מסמך זה עודכן לאחרונה בתאריך: [יש למלא את התאריך האחרון בו עודכן מסמך זה]