עודכן בנובמבר 2024

נספח הגנת מידע

[מיועד לשירות מיקור חוץ ו/או שירות הכרוך בעיבוד מידע]

בהתאם להוראות חוק הגנת הפרטיות, התשמ"א – 1981 ותקנותיו, לרבות ובמיוחד תקנות הגנת הפרטיות (אבטחת מידע) – התשע"ז 2017 והנחיות הרשות למשפט טכנולוגיה ומידע, נותן השירות הח"מ הינו מחזיק מאגר כהגדרתו בחוק ומתחייב כדלהלן:

1. נספח זה הינו חלק בלתי נפרד מן ההסכם.
2. הגדרות עיקריות:
   2.1 דיני הגנת הפרטיות הרלוונטיים משמעם לרבות אך מבלי לגרוע מכלליות האמור, חוק הגנת הפרטיות התשמ"א 1981, תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, הנחיה מס' 2/2011 מאת רשם מאגרי המידע בנוגע לשימוש במיקור חוץ וכל הנחיה ו/או נוהל ו/או חוזר רלוונטי כפי שיהיו בתוקף מעת לעת.
   2.2 מושא נתונים – אדם מזוהה או הניתן לזיהוי במישרין ו/או בעקיפין.
   2.3 מידע ו/או מידע רגיש – כהגדרתם בחוק הגנת הפרטיות
   2.4 עיבוד מידע – כל פעולה או מערכת של פעולות המבוצעות על נתונים אישיים או על קבוצות של נתונים אישיים, בין אם באמצעים אוטומטיים, כגון איסוף, הקלטה, ארגון, בנייה, אחסון, הסתגלות או שינוי, אחזור, ייעוץ, שימוש, גילוי על ידי שידור, הפצה או ביצוע בדרך אחרת, יישור או שילוב, הגבלה, מחיקה או הרס.
3. נותן השירות מתחייב כי יעשה שימוש במידע אך ורק לשם המטרה המוגדרת בהסכם ואך ורק על ידי עובדים מטעמו בעלי הרשאה למידע כפי שהוסכמו בין נותן השירות לקבוצת שירותי בריאות כללית (כללית על כל גופיה, מוסדותיה, חברות הבת ו/או חברות נכדות) (להלן: "כללית").
4. נותן השירות מצהיר כי ידוע לו כי המידע לרבות מידע אשר יעובד במערכות של כללית או מידע עבור הכללית שהספק ייצר במסגרת התקשרות זו, הוא בבעלותה הבלעדית של כללית, וכי לנותן השירות לא יהיה רשאי לעשות בו כל שימוש שאינו לצורך ביצוע ההתקשרות עם כללית על פי הסכם זה.
5. נותן השירות מתחייב להגיש לאישור הממונה על הגנת המידע את טופולוגית מערכות המידע / המחשוב / רשת ותקשורת / אינטרנט / גישה מרחוק וכו' כולל אמצעי הגנת ואבטחת המידע הקיימים אצלו.
6. נותן השירות ינהל את ההרשאות במערכת באמצעות מודול הרשאות אשר יאפשר גישה למידע רק לבעלי ההרשאות בהתאם לתפקידם ולהסיר משתמשים אשר סיימו עבודתם או שעברו לתפקיד אחר אשר אינו מחייב הרשאת גישה על פי הסכם זה.
7. הרשאה כאמור למידע רפואי אישי או מידע עסקי רגיש תיעשה רק לאחר הזדהות אישית חזקה.

8. מבלי לגרוע מאחריות נותן השירות על פי נספח זה נותן השירות מתחייב להחתים כל עובד/ת או מי מטעמו אשר מעורב בביצוע ההסכם, קודם לתחילת עבודתו עבור כללית, על התחייבות אישית לשמירת סודיות והגנת מידע בנוסח אשר עומד בדרישות נספח זה.
במקרה בו עובד של החברה מוצב במתקני הכללית או שמונפק לו שם משתמש על ידי הכללית, יחתום העובד על הצהרת סודיות בנוסח הנהוג בכללית לעובדי כללית.
9. מערכות המאגר יתעדו כל גישה / עדכון / מחיקה של מידע בגישה למאגר במנגנון לוג מתאים הכולל את שם המשתמש, תאריך, שעה, כתובת ה IP של התחנה ממנה נגש וכן את הפעולה שביצע במערכת כולל זיהוי חד חד ערכי של נשוא המידע.
10. נותן השירות מתחייב כי לא יעביר, בתמורה ו/א ושלא בתמורה לכל גורם צד שלישי מידע מכל מין וסוג שהוא אשר הגיע אל נותן השירות במסגרת הסכם זה.
11. נותן השירות מתחייב להדריך את העובדים מטעמו ו/או עבורו ו/או שלוחיו בכל הנוגע למטרת השימוש במידע ואופן השימוש בהרשאות על ידי המורשים לכך.
12. בעת איסוף מידע ישירות על ידי נותן השירות מאת נשוא המידע – יפעל נותן השירות בהתאם לכל הוראות חוק הגנת הפרטיות התשמ"א 1981 לרבות ובמיוחד מתן הסבר מפורט לנשוא המידע בדבר מטרת איסוף המידע, אופן השימוש והשמירה שלו.
13. נותן השירות מתחייב בזאת כי לא יאסוף מידע, במישרין ו/א ובעקיפין ולא ינסה לאסוף מידע על נשואי המידע אלא בדרכים הקבועות בהסכם זה ולא יעשה שימוש בכל מאגר מידע בלתי חוקי.
14. נותן השירות מתחייב כי כלל הרכיבים, אשר נעשה בהם שימוש על ידי נותן השירות במסגרת התקשרותו עם כללית, עומדים בדרישות בחוק הגנת הפרטיות ותקנותיו ובכל החלטות הממשלה.
15. נותן השירות מתחייב כי אם השירות ניתן באמצעות מכשור המתחבר למערכות מחשוב בהן קיים מידע רגיש או אישי או אם המכשיר אוסף מידע רגיש או אישי, נותן השירות יעשה שימוש באמצעים מאובטחים בלבד.
16. בהסכם בו אושר חיבור לרשת הכללית או למערכות המידע של כללית, החיבור ייעשה בהתאם להנחיות הממונה על הגנת המידע בכללית.
17. נותן השירות מתחייב שלא יבצע כל שינוי הגדרות או אחר בכל רכיבי חומרה או תוכנה המתחברים לכללית או מחזיקים מידע של הכללית או של לקוחות הכללית ללא אישור מראש ובכתב מהממונה על הגנת המידע בכללית.
18. נותן השירות מתחייב לבצע על חשבונו עדכון גרסה או שדרוג במערכות המידע שלו ו/או בתשתיות המחשוב שלו במקרה ששינוי בהגנת מידע או טיפול באיום על הגנת המידע יחייב, לדעת הממונה על הגנת המידע בכללית, ביצוע עדכון כאמור.
19. נותן השירות מתחייב לבצע על חשבונו פעם ב 18 חודשים לכל הפחות, בדיקת חוסן penetration test וסקר סיכונים למערכות המחשוב ולמאגרי המידע אצלו ולכל מערכות המידע שלו הקשורים בהסכם זה או המחזיקים / נגישים למידע של ועל מבוטחי הכללית. נותן השירות מתחייב שהבדיקה תבוצע עלי ידי חברת אבטחת מידע חיצונית מוכרת ומקובלת בשוק. נותן השירות יעביר את תוצאות בדיקת החוסן אל הממונה על הגנת המידע בכללית. נותן השירות מתחייב להתאים את המערכת על חשבונו למלוא הדרישות כאמור מתוצאות בדיקת החוסן.

20. נותן השירות מתחייב לערוך פעם ב 24 חודשים, לכל הפחות, ביקורת פנימית או חיצונית על ידי גורם בלתי תלוי בעל הכשרה מתאימה לביקורת אבטחת מידע (שאינו הממונה על אבטחת המידע של נותן השירות) לווידוא עמידת נותן השירות בהוראות תקנות הגנת הפרטיות. נותן השירות יעביר דוח זה לממונה הגנת המידע בכללית.
21. נותן השירות מתחייב לעמוד בתקן ISO 27001 כפי שנדרש בחוזר מנכ"ל משרד הבריאות מס' 3/15 ו/או בכל הוראת דין אחרת כפי שתהא בתוקף מעת לעת.
22. על נותן השירות להעביר לידי הממונה על הגנת המידע בכללית את דו"ח מבקר ISO לעמידה בתקן ISO 27001 אחת לשנה, כולל התייחסות נותן השירות לאי ההתאמות שהועלו במבדק.
23. נותן השירות מתחייב כי אם הוא מספק שירותים למספר מזמינים שונים, יפעל בהתאם לקבוע בסעיף 17א' לחוק הגנת הפרטיות.
24. נותן השירות מצהיר כי ידוע לו שאם לצורך מתן השירות נדרשת גישה למערכות המידע של הכללית, נותן השירות יקים קו תקשורת בין החברה לכללית ואזור ממודר, פיזית ותקשורתית, אשר יהיה מופרד לחלוטין מרשת התקשורת של נותן השירות ועל פי דרישות הגנת המידע של הממונה על הגנת המידע בכללית.
25. נותן השירות יספק למזמין דיווח שוטף בכל הנוגע לאופן ניהול מאגר המידע ועיבוד המידע.
26. נותן השירות ידווח למזמין מיד בכל מקרה של חשש לדליפת מידע מהמאגר או שימוש חורג מההרשאה שניתנה.
27. מבלי לגרוע מחובות נותן השירות כאמור, המזמין שומר לעצמו את הזכות לערוך ביקורות באתר נותן השירות, לרבות ביקורות פתע, לצורך בחינת אופן התנהלות נותן השירות בסוגיות איסוף המידע ואבטחתו.
28. נותן השירות יעביר הדרכה לעובדיו ו/או שלוחיו בכל הנוגע לעקרונות הסכם זה בדבר אבטחת המידע וכן הדרכות ריענון פעם בשנתיים.
29. נותן השירות מתחייב כי בתום סיום ההתקשרות על פי הסכם זה יעביר כל מידע השייך לכללית ו/או נאסף ו/או עובד עבורה ולאחר מכן ימחק כל מידע כאמור מכל אמצעי המדיה שברשותו ו/או אמצעי גיבוי ו/או כל מדיה מגנטית או אופטית אחרת וזאת למעט במקרה בו נדרשת שמירה על פי דין. נותן השירות מתחייב כי יספק למזמין תצהיר המאמת את ביצוע פעולות המחיקה, ביעור והשמדה של כל המידע כאמור.
30. נותן השירותים מתחייב כי אם הוא עושה שימוש בשירותי ענן (Cloud) עבור שירותיה לכללית, שירותים אלו יאובטחו בהתאם לסטנדרטים המקובלים בעולם ולהמלצות הרשות להגנת הסייבר. בכל מקרה מידע רגיש על פי הגדרות החוק יוצפן בענן. שירותי הענן ימצאו בגבולות הגיאוגרפיים הניתנים במדינת ישראל ו/או במדינות הנמצאות בתחומי האיחוד האירופאי וחתומות על האמנה האירופאית להגנה על שמירת הפרטיות והמידע.
31. נותן השירותים מתחייב לאבטח את תחנות הקצה מהם ניגשים למאגר בהתאם לסטנדרטים המקובלים בעולם ולהמלצות הרשות להגנת הסייבר כפי שיעודכנו מעת לעת.
32. נותן השירותים מתחייב לאבטח את רשת התקשורת והתשתיות שלו ובנוסף את חיבורי האינטרנט החיבורים האלחוטיים ואמצעי הגישה מרחוק בהתאם לסטנדרטים המקובלים בעולם ולהמלצות הרשות להגנת הסייבר. כפי שיעודכנו מעת לעת.

33. נותן השירותים מתחייב לעמוד בכל הוראות הדין לרבות חוק הגנת הפרטיות ותקנותיו.
34. נותן השירותים מתחייב לאבטח באופן פיזי את מאגר המידע, מחשבים שרתים בסיסי נתונים כך שלא יהיו נגישים לבלתי מורשים.

חובות נוספות בקשר להגנת פרטיות המידע ולאבטחתו

35. **גישה מרחוק למתן שירות ללקוח**: יובהר כי כל גישה מרחוק בין אם לתיקון תקלות ובין אם לשדרוג תוכנה – תיעשה **אך ורק לפי בקשה מפורשת של לקוח כללית ובאישור הלקוח**, שיתועדו על ידי הספק. גישה מרחוק כאמור, תיעשה אך ורק באמצעים מאובטחים, וכן בהזדהות חזקה, ובהתאם לדרישות האבטחה כמפורט **<u>בתוספת א'</u>**.

35.1 נותן השירות לא יאסוף כל מידע אישי מנושא המידע, למעט מידע טכני בלבד (שאינו כולל מידע אישי) הנחוץ באופן הכרחי לטיפול בתקלות או לפניות מטופל בקשר למתן השירותים. במקרה כזה הספק מתחייב לפעול לפי דרישות סעיף 11 לחוק הגנת הפרטיות, ובכלל זאת יסביר הספק לנושא המידע כי לא חלה עליו חובה חוקית למסור את המידע וכי מידע יימסר אך ורק מרצונו, את תוצאות סירובו למסור מידע, את מטרות מסירת המידע, את אופן שמירתו ולמי הוא יועבר.

35.2 **מתן הסבר ללקוח על מגבלות המערכת בתחום הפרטיות ואבטחת מידע והבאת מסמך לחתימתו:** נותן השירות יסביר ללקוח את מגבלות המערכת בתחומי הגנת פרטיות וחיסיון רפואי ואפשרות אירועי כשל תקשורתי בקשר למתן השירותים; כמו כן יסביר ללקוח בדבר אחריותו שלו לפרטיותו, לרבות לשמירת סודיות המידע הרפואי במחשב אישי, ומניעת אפשרות גישה למידע או לשירות למי שאינו מורשה לכך על ידו, וכיו"ב, ובין היתר כמפורט **<u>בתוספת א'</u>** לנספח זה להלן.

מבלי לגרוע מהאמור, **במועד אספקת הציוד כמפורט בהסכם זה לראשונה ללקוח, נותן השירות מתחייב להביא לחתימת הלקוח מסמך מטעם כללית**, שנועד בין היתר להבהיר ללקוח את אחריותו למידע המצוי במחשב המסופק לו. נותן השירות יבקש את אישורו וחתימתו של הלקוח על מסמך כאמור, ויעביר את המסמך החתום על ידי הלקוח בסמוך לאחר אספקת הציוד ללקוח, לכללית.

35.3 מבלי לגרוע מכלליות האמור לעיל, נותן השירות יבהיר ללקוח כי <u>אין</u> להעביר מידע אישי מכל סוג (לרבות במפורש מידע רפואי) במערך שירות הלקוחות, וכי אין להעביר כל מידע כזה בדוא"ל או בווטאסאפ.

אירועי אבטחת מידע ואירועי סייבר

36. נותן השירות מתחייב לדווח לכללית מיידית, בעל פה ובכתב, על כל אירוע אבטחת מידע ו/או סייבר ו/או חשש לאירוע כאמור ו/או החלטה בעניין אירוע כאמור, בכל אחד מהמקרים המפורטים מטה:

36.1 כל חשש לאירוע אבטחת מידע ו/או סייבר הנוגע במישרין או בעקיפין למידע לפי הסכם זה (לרבות מידע כללית ו/או מבוטחיה).

36.2 כל חשש לאירוע אבטחת מידע ו/או סייבר שיש בו כדי להשפיע על רמת אבטחת המערכת או שיש בו כדי להשפיע על רמת אבטחת מידע אצל נותן השירות, לרבות כל חשש לאירוע אבטחת מידע ו/או סייבר בקשר לתוכנה.

36.3 כל ליקוי אבטחת מידע מהותי (כגון תשתיתי, אפליקטיבי) אשר עלול להוביל לפגיעה בשלמות, סודיות וזמינות המידע אודות לקוחות כללית.

36.4 כל אירוע אבטחת מידע ו/או סייבר משמעותי אצל נותן השירות, לרבות בתשתיות ומערכות הספק ו/או בציודו ו/או במתקניו.

37. נותן השירות מתחייב כי בכל אחד מהמקרים האמורים לעיל, יודיע על כך מיידית בע"פ ובכתב לממונה הגנת מידע בכללית ו/או למוקד שירותי בריאות כללית (פרטי המוקד: מייל – SOC@clalit.org.il; טלפון – 03-694-5644) וישתף פעולה לאלתר עם הכללית לשם חקירה וטיפול באירוע כאמור.

38. הודעה (טלפונית ובכתב) בדבר אירוע אבטחת מידע / סייבר או חשש לאירוע כאמור לעיל תכלול מידע מפורט על אירוע האבטחה לרבות: תיאור האירוע, מידת ההשפעה על המידע ו/או על המערכת ו/או על תשתיות ומערכות הספק, ופעולות שננקטו על ידי נותן השירות. נותן השירות ימשיך ויעדכן את הכללית במהלך האירוע לפי ההתפתחויות, ולכל הפחות אחת ל – 24 שעות.

39. מבלי לגרוע מהאמור לעיל, באירוע אבטחת מידע ו/או סייבר אצל נותן השירות או בחשש לאירוע כאמור, שבו קיים חשש כי מעורבים מידע (לרבות מידע הכללית) ו/או המערכת ו/או תשתיות ומערכות הספק בהתאם לנספח זה, יפעל נותן השירות בהתאם לחובותיו על פי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017, ככל שקיימות בנסיבות המקרה, וזאת מבלי לגרוע ממחויבויותיו כלפי הכללית כמפורט בהסכם ובנספח זה.

40. זכויות נושאי מידע וטיפול בפניות נושאי מידע

40.1 קיבל נותן השירות פניה ישירה מנושא מידע, בכל הנוגע למידע לגביו הנמצא במאגרי המידע של הכללית ו/או המעובד בתשתיות ובמערכות נותן השירות, לרבות בקשר לזכות עיון, או בקשה הנוגעת לתיקון מידע, יעדכן נותן השירות את הכללית באופן מיידי, יעביר לה את הפנייה, ויפעל בתיאום עימה. אלא אם אושר לנותן השירות במפורש מראש ובכתב, הטיפול בפניות נושאי המידע יתבצע על ידי הכללית בלבד, ונותן השירות לא ישיב לפנייה בעצמו.

40.2 נותן השירות יסייע לכללית בטיפול בפניות של נושאי מידע ככל שתהיינה, וזאת מבלי לגרוע מיתר הוראות ההסכם ונספח זה, לרבות, אך לא רק, חובתו של נותן השירות להשמיד את המידע המועבר אליו בתום ההתקשרות, כמפורט בנספח זה. בכל מקרה בו תבקש כללית מנותן השירות לעדכן ו/או לשנות ו/או למחוק מידע – יפעל נותן השירות לאלתר על פי דרישת כללית.

41. נותן השירות מתחייב לשפות את הכללית מיד עם דרישתה הראשונה בגין כל נזק ו/או תביעה ו/או דרישה הנובעת ו/או הקשורה להפרת נותן השירות את התחייבותו לעמידה בכל כללי אבטחת המידע הן על פי הדין והן על פי הסכם זה וכי הוא מחזיק בביטוח בתוקף בחברת ביטוח מורשית כדין לפיצוי ושיפוי כאמור.

תאריך _____

שם החברה _____

שם החותם _____

מספר ת״ז _____

שם הפרויקט או השירות _____

חותמת וחתימת החברה_____