כ״ה בטבת, התשפ״ג
18/01/2023
סימוכין: 12093323
מס׳ פניה: 636903
סיון דדון
(בתשובתך ציין מספר פניה)

לכבוד
עו״ד אלעד מן עמותת הצלחה לקידום חברה הוגנת
foi@htl.org.il

שלום רב,

הנדון: בקשה לקבלת מידע במסגרת חוק חופש המידע – מעבדת מי הריטג׳

בפנייתך ביקשת לקבל את המידע הבא:

1. העתק ההסכם או ההסכמים, על נספחיהם, עם החברות MyHeritage ו-BGI (להלן ״החברות״ ו/או ״החברה״) וכן את מסמכי המכרז למתן שירותים או הפניה לקבלת הצעות למתן שירותים שבעקבותיהן נכרתו הסכמים אלו, במקביל לפרסומם ברבים.
2. פירוט אופן עיבוד מידע רפואי על-ידי מפעילת המעבדה הנוגעת להסכמים אלו והנהלים וההנחיות הנוגעים לעניין זה.
3. זהות הגורמים להם החברה רשאית להעביר מידע רפואי הנוגע לבדיקות ולנבדקים, וכל הוראה, נוהל או הנחיה בעניין זה בנוסף על האמור בהסכם ההתקשרות.
4. פרטים הנוגעים למשך הזמן במהלכו החברות הפרטיות מורשות לשמור מידע רפואי אודות נבדקים וכל הוראה, נוהל או הנחיה בעניין זה מעבר לאמור בהסכם ההתקשרות
5. פירוט ההגנות ואמצעי אבטחת המידע שעל חברות המפעילות מעבדות פרטיות לנקוט ביחס למידע רפואי של נבדקים והמסמך המעגן אותם לרבות כל הנחיה, נוהל והוראה בעניין זה.
6. פרטי החיבור בין מערכות החברה לבין מערכות קופות החולים על מנת לקבל מידע רפואי ו/או דגימות של נבדקים. אם כן, כיצד החברה מפרידה בין מידע שהתקבל מקופות החולים למידע של לקוחותיה, ופירוט אמצעי האבטחה שננקטים ביחס להעברה ואחסון המידע. כן נבקש לקבל כל נוהל, הנחיה ו/או הוראה בעניין זה.
7. פירוט אמצעי הבקרה של משרד הבריאות אל מול החברה במטרה למנוע אירועים של כשל באבטחת מידע, ולהבטיח עם התרחשותם טיפול מהיר ומקצועי בהן. פירוט כל פעולות בקרה שבוצעו עד כה כדי לוודא מהם אמצעי האבטחה שהחברה נוקטת ומה היו ממצאיהן ומהות הצעדים שננקטו בעקבות ממצאים אלו.
8. פירוט ההרשאות לחילוץ מידע, לרבות מידע גנטי מתוך נתוני הבדיקות המבוצעות ומנותחות וכן פירוט המטרות שלשמן מחולץ מידע זה.

לאחר בירור עם הגורמים המקצועיים במשרד להלן תשובתנו –

סעיף 1 - הופנית על ידינו לקבלת המידע ממשרד הביטחון והמידע נמסר לך על ידם.

סעיפים 2, 3 - מענה מופיע במסגרת הסכם ההתקשרות (סעיפים 3-4)

סעיף 4 - לאחר חתימת ההסכם, הונחתה המעבדה על ידי ממונה אבטחת מידע במשרד הבריאות על שמירת המידע במעבדה למשך 90 ימים לאחר מסירת תוצאות הבדיקה . רצ״ב הנחיה שנשלחה לספקי דיגום הקורונה בנושא מחיקת מידע שנאגר.

סעיף 5 - סעיף 3 להסכם ההתקשרות נותן מענה לשאלות סעיף 5. כמו כן רצ״ב לעניין זה נוהל פיתוח מערכות מאובטחות; הנחיות אבטחת מידע לספקים; מסמך פיתוח מאובטח ואבטחה בתהליכי פיתוח תמיכה ותחזוקת מערכות.

סעיף 6 – קיים ממשק בין קופות החולים למעבדה. הממשק הינו בטווח מוצפן באמצעות כספות על פי הנחיית משרד הבריאות.

ביחס להפרדת המידע שהתקבל מקופות החולים למידע של לקוחותיה נציין כי חברת My Heritage הקימה סביבת מעבדה הכוללת תשתיות מחשוב וציוד בקרה הכולל סגמנטציה מלאה לסביבת העבודה ,מערכות אבטחה ,חוקיות תצורת העבודה ,מגנוני הגנה ברמת תחנות עבודה והשרתים, איתור וניטור. סביבת רשת המעבדה לא מחוברת לאינטרנט מלבד הקישור לרשת משרד הבריאות שנעשה בצורה מאובטחת על בסיס משיכה בלבד ,ההגדרות מיושמות ברכיב ה FW -של המעבדה בצורה פרטנית. כמו כן, בוצעה הפרדה מלאה בצבעי כבלי התקשורת של המחשבים וציוד מעבדה בהתאם לסגמנטי העבודה.

באשר לפירוט אמצעי אבטחת המידע שננקטים ביחס להעברה ואחסון המידע נבהיר כפי שהוסבר לעיל, סביבת רשת המעבדה לא מחוברת לאינטרנט מלבד הקישור לרשת משרד הבריאות שנעשה בצורה מאובטחת על בסיס משיכה בלבד , ההגדרות מיושמות ברכיב ה FW -של המעבדה בצורה פרטנית.

סוגיות האבטחה הפיזית ,בקרת כניסה ומצלמות ביטחון למבנה הניהולי וגישה לחדרי המעבדות טופלו והוגדרו ברשת ייעודית הכוללת רכיבי בקרת כניסה ,כרטיסי RFID מצלמות וציוד הקלטה ,דלתות כפולות, כמו כן הוגדר קצין ביטחון האחראי לסידורי הביטחון במעבדה הנ"ל עם ניסיון של 16 שנים בעולם המעבדות הציוד והמכשור הרפואי.

תחנות העבודה ברשת המעבדה ומערכת השרתים הוגדרו לדיווח במערכת ה SIEM -הארגוני בחוק ייחודי ורגיש וכל התרעה שתעלה ממחשבים אלו תדווח למנהל אבטחת המידע ולצוות התשתיות ותטופל במיידית ע"י הגורמים הרלוונטיים בחברה ,במידה וקיימים צבר אירועים חריגים נדרש לדווח ל SOC -מגזר הבריאות.

חסימת שקעי USB למניעת הכנסת DOK או כל חיבור אחר למחשבי המעבדה נדרש לביצוע.

בוצעה הפרדה מלאה בצבעי כבלי התקשורת של המחשבים וציוד מעבדה בהתאם לסגמנטי העבודה.

ע"פ חברת My Heritage, לא מתוכננת גישת תחזוקה חיצונית מרוחקת למכונות ע"י גורמי חוץ ,תחזוקה תבוצע בצורה מקומית ע"י החברה או חברת אחזקה שאיתה חתמה My Heritage על חוזה תמיכה בליווי צמוד או גורמי התשתיות של החברה.

סעיף 7 - תהליכי הבקרה וההנחיה שבוצעו בתחום אבטחת המידע והגנת סייבר עבור My Heritage בתחום הדיגום והמעבדות זכו במכרז להפעלת מערך ביצוע דגימות לאיתור נשאי נגיף הקורונה עבור משרד הבריאות. המכרז גובש על-פי דרישות משרד הבריאות, תהליך הליווי והבדיקה בוצעו במטרה להנחות לגבי דרישות אבטחת המידע כפועל יוצא מדרישות המכרז ובמטרה לאמוד את מידת אבטחת המידע של מעבדת הקורונה החדשה. המשרד איגד דו״ח בדיקת ספקים אשר מפרט את כלל הממצאים, הסיכונים, החשיפות וההמלצות שאותרו למול הספקים לביצוע בדיקות חדירות וליווי ע״י חברות אבטחת מידע והגנת סייבר ע״מ להבטיח את בטחון המידע הרפואי ואישי המוחזק בדיקה ראשונית בוצעה בחודשים אוקטובר- נובמבר , 2020.

הסקר בוצע ע״י יחידת ההנחיה בסייבר של משרד הבריאות באמצעות תשאול ספקים והצהרה על קיום תהליכי אבטחת מידע בכללם בדיקות חדירות עצמאיות אשר מהוות נספח למבדק התהליכי והצהרה של קיום התחייבויות אלו עבור כלל ספקי המשנה בפרויקט מצד הספק.

תהליך הבקרה כלל בדיקה מקיפה של ארכיטקטורת ומתווה הפתרון כדלקמן:

1. הרשאות המערכת ובעלי התפקידים הרשאים לגשת למידע – פונקציות עיקריות
2. RPO/RTO עבור שרידות המערכת וזמן השחזור הנדרש
3. שאלון ספקים והצהרה על התהליכים לאבטחת המידע והגנת הסייבר ותיקוף דרישות המכרז בהתאם לקובץ שרשרת אספקה משרד הבריאות ומערך הסייבר הלאומי.
4. מתווה לבדיקות חדירות והצגת השלבים לפני עלייה לאוויר
5. בקרה של התהליך ע״י משרד הבריאות במשרדי הארגון הנסקר

חברת MyHeritage החלה את פעילותה לאחר אישור לפעילות של מערך הסייבר הלאומי שבדק את ציוד המעבדה ואישר את פעילות המעבדה וכן בוצעה העברת מקל בין מערך הסייבר ליחידה המגזרית במשרד הבריאות.

עם סיום המכרז, המעבדה עברה בקרה של ערך הסייבר ובהמשך משרד הבריאות ערך למעבדה בקרות אבטחת מידע וסייבר.
כיום המשרד מפעיל מנגנוני מודיעין סייבר בכדי לאתר אירועי אבטחת מידע וסייבר – עד כה לא נמצאו ממצאים המצביעים על אירועי אבטחת מידע במעבדה
בנוסף המשרד מחייב את המעבדה לעמוד בתקן ISO 27001 אבטחת מידע והקצה לכך 12 חודשים מרגע חתימה ההסכם כתנאי להמשך פעילות.

<u>סעיף 8 –</u> תוך כדי בקרה שבוצעה על ידי מחלקת אבטחת מידע במשרד הבריאות, נבדק נושא ההרשאות ונמצא כי המערכת כוללת פרופילי הרשאה (צפייה/קריאה/כתיבה)ברמת השדה במערכת וכוללת מימוש מנגנון . RBAC/ABAC, , במערכת eL@b קיימות הרשאות מבוססות RBAC בנוסף לשימוש מוסדר בקבוצות ב Active Directory

החברה אינה מורשית לחלץ מידע גנטי.

הנני להודיעך כי לפי סעיף 17 לחוק חופש המידע יש בידך לעתור כנגד החלטה זו לבית המשפט לענייניים מנהליים בירושלים, בתוך 45 יום.

בכבוד רב

סיון דדון, עו״ד
מ״מ ממונה על חוק חופש המידע