21 ינואר 2021
ח' שבט תשפ"א

דגשים והמלצות להגנת הפרטיות בבחינות מרחוק הכוללות אמצעים לשמירה על טוהר הבחינה במוסדות להשכלה גבוהה

מבוא

1. בחינות מרחוק הן בחינות המתקיימות באמצעות מערכות טכנולוגיות ייעודיות, המאפשרות לנבחנים להיבחן מכל מקום ובכל עת, לרבות ממדינה שונה מהמדינה בה נמצא המוסד האקדמי וזאת באופן המבטיח את טוהר הבחינה.
2. משבר הקורונה העולמי, אשר הוביל להטלת סגרים, מגבלות דרמטיות על התקהלות במקומות סגורים והנחיות לשמירה על ריחוק חברתי, אשר הוטלו על הציבור כאמצעים להתמודדות עם המגיפה, האיץ את המעבר ללימודים ולבחינות מרחוק במוסדות להשכלה גבוהה ונראה כי שינוי משמעותי זה יישאר, ולו בחלקו, גם לאחר תום המשבר.
3. במסגרת הצעדים שנקטה הממשלה בהתמודדות עם המשבר, הורה משרד הבריאות בצו על הגבלת קיומן של בחינות פרונטליות בנוכחות פיזית של סטודנטים, וקבע כי ניתן לקיימן רק בהתאם להוראות פרטניות של המועצה להשכלה גבוהה.[1] מציאות זו גרמה לכך שמוסדות להשכלה גבוהה בישראל נדרשו למצוא חלופות לקיומן של בחינות פרונטליות, ובחלק מהמקרים החלופה שנבחרה היא קיום בחינות מרחוק באופן מקוון.
4. כפי שנסביר במסמך זה, לצד היתרונות הגלומים בבחינות מרחוק קיימים גם חסרונות לשיטה זו המעלה מצד אחד חשש לפגיעה בפרטיות הנבחנים, ומן העבר השני חשש לפגיעה בטוהר הבחינה, כאשר במקרים רבים אותן מערכות מקוונות המאפשרות קיומן של בחינות מרחוק כוללות גם אמצעים דיגיטליים אשר מטרתם לשמור על טוהר הבחינה. אמצעים אלה מאיימים על פרטיות הנבחן שכן הם אוספים מידע אישי על אודותיו, ופגיעה במידע זה או חשיפתו לציבור עלולה לגרום נזק רב לנבחן ולמוסד. ואכן, בעקבות השימוש בטכנולוגיות אלו על ידי מוסדות להשכלה גבוהה ברחבי הארץ, התקבלו ברשות להגנת הפרטיות תלונות רבות מצד סטודנטים המתייחסות לפרקטיקה זו.

[1] ראו סעיף 2א(א1) לצו בריאות העם (נגיף הקורונה החדש)(הגבלת פעילות מוסדות חינוך)(הוראת שעה), התש"ף-2020. ראו גם החלטת המועצה להשכלה גבוהה מיום 9.7.20, בה נקבע כי מבחנים בנוכחות פיזית במוסדות יתקיימו אך ורק במקרים חריגים ולא יותר מ-10% מסך הבחינות ובהתאם לנוהל הבחינות אשר פורסם על ידי משרד הבריאות:
https://che.org.il/wp-content/uploads/2020/09/%D7%94%D7%97%D7%9C%D7%98%D7%95%D7%AA-%D7%9E%D7%95%D7%A2%D7%A6%D7%94-9.7.2020.pdf
החלטה זו אף היא כפופה למגבלות על נוכחות פיזית במוסדות חינוך ועל התקהלות במקום סגור, המוטלות מעת לעת על ידי הממשלה בהתאם לרמת התחלואה בנגיף הקורונה. ראו סעיף 10(ד) לחוק סמכויות מיוחדות להתמודדות עם נגיף הקורונה החדש (הוראת שעה), תש"ף-2020.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

5. **מטרת מסמך זה הינה לתת דגשים והמלצות להגנת פרטיות הנבחנים בעת ביצוע בחינות מרחוק הכוללות אמצעים להבטחת טוהר הבחינה במוסדות להשכלה גבוהה, בראי הצורך לשמור על טוהר הבחינות, על רמה אקדמית נאותה ועל החופש האקדמי של המוסדות.**
6. יודגש כי מאחר שמדובר בטכנולוגיה אשר השימוש בה בארץ חדש יחסית, הדגשים ראשוניים בלבד. הרשות עשויה לשוב ולבחון את השימושים במערכות אלה, וייתכן כי תפרסם הנחיות ודגשים נוספים בעתיד.
7. המלצות אלה אינן גורעות מהוראות כל דין ויש לקרוא אותן לאור הוראות חוק הגנת הפרטיות התשמ"א-1981, התקנות אשר הותקנו מכוחו, והנחיות הרשות להגנת הפרטיות.

<u>מאפיינים טכנולוגיים של בחינות מרחוק</u>

<u>סוגים של בחינות מרחוק</u>

8. כאמור, בחינות מרחוק מאפשרות לנבחנים הנמצאים באזורים גיאוגרפיים שונים מהמקום שבו ממוקם המוסד האקדמי להשתתף בבחינות, מבלי להגיע פיזית למוסד. כפי שנדגים בהמשך, המערכות בהן מסמך זה עוסק נסמכות, בין היתר, על צילומי וידאו של הנבחן וסביבתו ועל אמצעים נוספים שנועדו למנוע מעשי מרמה והעתקות, ובכך להבטיח את טוהר הבחינה.
9. ישנן מערכות טכנולוגיות שונות המאפשרות לבצע בחינות מרחוק תוך שמירה על טוהר הבחינה, כאשר כל מוסד אקדמי בוחר את ספק השירותים והמערכות עימם הוא מבקש להתקשר. מאפייניו המדויקים של השירות משתנים מספק שירות אחד למשנהו, אולם ניתן לסווג את המתכונת שבה נערכים המבחנים מרחוק לשלוש קטגוריות עיקריות:[2]

<u>פיקוח בזמן אמת</u> - במתכונת זו, המשגיח על הבחינה מפקח על הנבחנים מרחוק, משך כל זמן הבחינה. למשגיח יש יכולת להתערב במהלך הבחינה, ולפנות אל הנבחן ישירות (לרבות כדי להתריע על מעשים בלתי חוקיים). מתכונת זו דורשת תיאום הבחינה למועד מסוים (קרי, לנבחן אין אפשרות לבחור את המועד שבו נוח לו להיבחן), וישנה כמות מוגבלת של מסכים עליהם משגיח מסוגל לפקח בו זמנית.

<u>אחסון צילומי הבחינה ופיקוח במועד מאוחר יותר</u> - בשיטה זו צילומי הווידאו נשמרים, והמשגיח בוחן אותם בתום הבחינה. על סמך הצילום המשגיח יעריך אם בוצעה פעולה בלתי חוקית או לא. שיטה זו מאפשרת לנבחן לגשת לבחינה מבלי שיהיה צורך לתזמן את הבחינה מראש ומבלי להכפיף את קיומה לזמינותם של משגיחים. חסרונה של שיטה זו הוא בכך שאין קשר ישיר בין הנבחן למשגיח, אשר אינו יכול להתריע בפני הנבחן, בזמן אמת, כי הוא מבצע פעולות לא חוקיות.

[2] https://www.surf.nl/files/2019-04/whitepaper-online-proctoring_en.pdf.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

פיקוח אוטומטי - בשיטה זו המערכת מזהה מקרים בהם קיימת הסתברות לכך שבוצעה הונאה של נבחן (המערכת מזהה למשל פתיחה של קבצים או תוכנות על מחשב הנבחן, הסטת מבט של הנבחן, נוכחות אדם נוסף בחדר בו שוהה הנבחן ועוד). המערכת מתריעה בפני המשגיח על קיום חשש להונאה, והוא יכול לעבור על הצילום בזמן אמת כדי להעריך האם באמת התבצעה הונאה. שיטה זו מייעלת את תהליך הפיקוח על הבחינה וחוסכת זמן בכך שמייתרת את הצורך לצפות בכל נבחן ונבחן, מתחילתה ועד סופה של הבחינה.

אמצעים לשמירה על טוהר הבחינה ולמניעת העתקות והונאות בבחינה מרחוק

10. השיטות להעתקות והונאות הן רבות, והחשש לפגיעה בטוהר הבחינה גובר כאשר הבחינות נערכות במתכונת מקוונת מרחוק, שכן בחינות אלה מתאפיינות בכך שהנבחן מבצע אותן באמצעות המחשב האישי שלו. הונאות יכולות להתבצע ע"י פתיחת דפדפן נוסף, סיוע של אדם שלישי המקבל גישה למחשב או נמצא בחדר בו שוהה הנבחן, תוכנות המשיבות למבחן במקום הנבחן עצמו, שימוש בפתקים ועוד. לצורך כך, מערכות לבחינה מרחוק מציעות מגוון רחב של אמצעים במטרה למנוע התנהגויות פסולות, לאתרן ובכך להבטיח את טוהר הבחינה.
11. להלן רשימה חלקית של סוגי אמצעים המשמשים לזיהוי הנבחן ולמניעת העתקות ומעשי תרמית (להלן: "אמצעים לשמירה על טוהר הבחינה"):[3]

מצלמות ומיקרופונים - מערכות רבות נסמכות על מצלמת הרשת של הנבחן, כדי לאפשר למשגיחים לפקח על מהלך הבחינה. במקרים רבים נעשה שימוש במצלמה נוספת, בדרך כלל המצלמה בטלפון הנייד או בטאבלט של הנבחן. המצלמה הנוספת בדרך כלל ממוקמת מאחורי הנבחן. השימוש במצלמות מאפשר למשגיח לצפות בחלק נרחב מהסביבה בה הנבחן מבצע את הבחינה, וכן לראות את המקלדת, העכבר והמסך.

שיתוף מסך - שיתוף מסך עם המשגיח מאפשר לו לצפות במסך ולראות אילו תוכנות פתוחות והאם הנבחן משתמש במקורות מידע אסורים.

נעילת דפדפן - אמצעי זה מונע שימוש בכל התוכנות האחרות במחשבו של הנבחן, למעט ממשק הבחינה עצמה והאפליקציות אשר השימוש בהן בזמן הבחינה אושר מראש.

לוגים במחשב - קיימות מערכות טכנולוגיות המותקנות על מחשבו של הנבחן ובכך מאפשרות לעקוב אחר פעולות במחשב. כדי להפעיל טכנולוגיות מסוג זה יש לקבל גישה מלאה למחשבו של הנבחן.

זיהוי תרמית ע"י ניתוח אופן ההקשה על המקלדת - ניתן לזהות נבחנים באמצעות סיסמה או ע"י האופן שבו הסיסמה מוקשת, קרי בדרך של הזדהות ביומטרית. שיטה זו נועדה לזהות מקרים בהם מי שמשיב לבחינה אינו הנבחן עצמו. אמצעי זה אינו מדויק לצורך קביעת הזהות הפוזיטיבית של המשתמש, אולם הוא יעיל לצורך פסילת זהות (קרי, לצורך קביעה כי מי שהקיש את הסיסמה אינו המשתמש הרשום). כאשר שיטת ההקלדה של הנבחן ידועה, המערכת תתריע אם וכאשר מי שמקליד על המחשב אינו הנבחן עצמו.

[3] שם, עמ' 26-27.

PPA@justice.gov.il | 02-6467064 | 073-3928555
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

שיטה זו מאפשרת להתגבר על החשש כי אדם נוסף אשר התחבר עם מקלדת נוספת הוא זה אשר משיב לבחינה במקום הנבחן. בהקשר זה נדגיש כי שיטת הקלדה עשויה להוות מידע ביומטרי רגיש.

טכנולוגיות זיהוי פנים - המערכת מזהה את פני הנבחן. ככל שאדם אחר כותב את הבחינה לאחר תהליך הזיהוי, המערכת תזהה ותתריע על כך.[4]

זיהוי תרמית ע"י אלגוריתם המנתח את תשובות הנבחנים - שימוש באלגוריתם אשר מנתח חשש להעתקה, במקרים של תשובות דומות.

כפי שנפרט להלן, אמצעים טכנולוגיים לשמירה על טוהר הבחינה אוספים מידע אישי על אודות הנבחן. לכן, ככל שנעשה שימוש באמצעים האוספים מידע רב יותר, לשם מניעת מרמה והעתקות, פגיעתם בפרטיות התלמידים קשה יותר.

סיכונים לפרטיות הנבחנים מרחוק

12. אמצעים לשמירה על טוהר הבחינה הינם בעלי פוטנציאל לאיסוף מידע אישי רב, כגון שם הנבחן, צילום תעודת זהות, כתובת IP, התנהגות הנבחן, מידע אודות סביבת הבחינה (מיקום, צילום סביבת הבחינה, הקלטת רעשים וכד'), מידע ביומטרי אודותיו (צילומי וידאו, תנועות ידיים, הבעות פנים, אופן ההקשה על המקלדת), ועוד. בנוסף, מצילומי הווידאו של הנבחן וסביבתו, ניתן ללמוד רבות אודותיו, לרבות מצבו הבריאותי (האם מרכיב משקפיים, עוויתות, טיקים בפנים ועוד), אמונתו (כיסוי ראש, ענידת סמלי דת אחרים), מוצא אתני ובמקרים מסוימים אף דעות פוליטיות ונטייה מינית (ככל שסביבת החדר בה הוא מצולם כוללת אינדיקציות לאלו). מלבד מידע אשר נאסף באופן גלוי כאמור לעיל, מתיעוד מהלך המבחן ניתן ללמוד רבות אודות כישורי הנבחן, כגון כמה זמן הוקדש לקריאת שאלה ומתן תשובה לשאלות מסוימות, לקויות למידה ועוד.

13. סיכון משמעותי נוסף מתעורר במקרים שבהם נעשה שימוש בטכנולוגיות המאפשרות גישה למידע המצוי במחשבו של הנבחן, שכן במחשב אישי מאוחסן מידע אישי עצום הכולל בין היתר תכתובות (מיילים, צ'טים במסנג'ר ובאפליקציות הרבות אשר הותקנו בו), תמונות, מסמכים אישיים, רשימת אנשי קשר, והרשימה כמובן עוד ארוכה. שימוש אסור במידע זה או פריצה אליו, עלולים לגרום לגילוי מידע אישי רב אודות הנבחן.

14. שילוב כל המידע האמור עם טכניקות של ניתוח נתונים, בינה מלאכותית והצלבה עם מידע אחר (למשל מידע המפורסם ברשתות החברתיות), מאפשר יצירת תמונה הכוללת מידע רב אודות הנבחן, ואף לשמש לניבוי עתיד מקצועי, מצב כלכלי עתידי ועוד. במידע זה ניתן לעשות שימוש אגרגטיבי לצרכי מסחר ואף ניתן להשתמש בו כדי לייצר פרופילים של נבחנים, להם קיים ביקוש רב בשוק סחר המידע.

[4] https://news.bloomberglaw.com/tech-and-telecom-law/student-proctoring-software-gets-first-test-under-eu-privacy-law.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

בשל הערך הרב של המידע, קיימת אפשרות כי ייעשה בו שימוש לרעה. שילוב של מידע ביומטרי (לרבות צילומי וידיאו) עם צילום תעודת הזהות אף מייצר סיכון לגניבת זהות.

15. **מהאמור לעיל עולה כי שימוש באמצעים טכנולוגיים לשמירה על טוהר הבחינה עלול להוביל לפגיעה קשה בפרטיות הנבחנים.**

16. בפרק הבא נציע מודל לאיזון בין סוג האמצעים הטכנולוגיים שבשימוש, חשיבות הבחינה, והעמדת חלופות ראויות עבור הנבחן, בכדי להגן על פרטיות הנבחנים תוך שמירה על טוהר הבחינה והחופש האקדמי של המוסדות להשכלה גבוהה.

<u>החלופות והשיקולים בעת בחירת מתכונת הבחינה והאמצעים לשמירה על טוהר הבחינה</u>

17. בשל ההשפעה המשמעותית של אמצעים לשמירה על טוהר הבחינה המתקיימת מרחוק על פרטיותו של הנבחן, מומלץ כי בהעדר אפשרות לקיים בחינה פרונטלית המוסד האקדמי ישקול בין השאר האם קיימת חלופה לעצם קיום הבחינה, שתאפשר לקבוע כי הנבחן עמד בחובות הקורס ומתן ציון, **מבלי לקיימה במתכונת של בחינה מרחוק הכוללת אמצעים טכנולוגיים מחמירים לשמירה על טוהר הבחינה**.

18. החלופות האפשריות לקיום בחינה מרחוק תלויות באופיו של המקצוע והשיעור, במתכונתו, במרצה, והן כוללות, בין היתר, חיבורים, מבחנים בעל פה, מבחנים המבוססים על אמון ללא פיקוח, כתיבת בחינה ולאחר מכן מתן מענה בעל פה, קיום בחינה פרונטלית בקפסולות, קיום בחינה במתכונת מפוצלת שתאפשר לנבחנים המעוניינים בכך להגיע פיזית למוסד האקדמי בזמן שהאחרים נבחנים באופן מקוון, תמהיל אחר של מטלות ובחינות על פי שיקול דעת המוסד האקדמי, דחיית הבחינה למועד אחר שיאפשר את קיומה באופן פרונטלי ועוד.

19. ככל שבנסיבות העניין המוסד האקדמי הגיע למסקנה, במסגרת שיקול הדעת האקדמי, כי לא ניתן להבטיח שמירה על רמה אקדמית נאותה באמצעות חלופות אחרות מלבד קיום הבחינה מרחוק תוך שימוש באמצעי לשמירה על טוהר הבחינה, **יש לבחור את האמצעי המידתי ביותר לצורך זה**, באופן שלא ימנע בפועל מהנבחן להיבחן, ושפגיעתו בפרטיות הנבחן תהיה מינימלית. בבחינת המידתיות יש לבדוק האם האמצעי אשר נבחר מגשים את המטרה, דהיינו האם הכלי שנבחר לשמירה על טוהר הבחינה הוא הכלי הטכנולוגי שפגיעתו בפרטיות היא המידתית ביותר בנסיבות העניין.

20. לצורך קבלת ההחלטה האם לקיים בחינה מרחוק, ומה הם האמצעים לשמירה על טוהר הבחינה שיוטמעו בבחינה הספציפית, מוצע לאזן בין מספר שיקולים ובין היתר:

<u>חשיבות הבחינה לציון הכללי בקורס</u> - לדוגמא בחינת הסמכה, בחינה מסכמת בקורס חובה וכו'.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

רמת החשש להעתקה ותרמית - במבחן רב-ברירתי ("מבחן אמריקאי") או מבחן הכולל שאלות קצרות להן תשובה אחת, הסכנה להעתקה גבוהה לעומת שאלות פתוחות המחייבות כתיבה ארוכה ומחשבה מקורית, בהן הסיכון להעתקה נמוך יותר וממילא קל יותר לזהותה.

עוצמת הפגיעה בפרטיות והיקף הגישה למידע אישי הניתן לאמצעי המשמש לשמירה על טוהר הבחינה, והאם ישנה חלופה טכנולוגית המשיגה המטרה תוך פגיעה פחותה בפרטיות. במקרים המתאימים, ניתן לשקול לבחור בחלופות כדוגמת אלה המנויות בפסקה 18 לעיל.

21. מדיניות פרטיות - מומלץ שכל מוסד אקדמי ינסח ויפרסם במסגרת מדיניות הפרטיות, הסדרה בנושא יישום אמצעים טכנולוגיים לשמירה על טוהר בחינות מרחוק, וזאת לאחר התייעצות עם כל הגורמים הנוגעים בדבר, לרבות ממונה הגנת הפרטיות של המוסד (אם ישנו כזה), ממונה אבטחת המידע של המוסד, היועץ המשפטי, ונציגי הסטודנטים.
22. שקיפות - מבלי לגרוע מהאמור לעיל, מומלץ לשקף את הנימוקים ותהליך קבלת ההחלטה באשר למתכונתן של הבחינות ואת האמצעים לשמירה על טוהר הבחינה עליהם הוחלט, כמו גם את אמצעי אבטחת המידע בהם משתמש המוסד האקדמי כדי להגן על המידע.

הבסיס החוקי לקיום בחינות מרחוק תוך שימוש באמצעים טכנולוגיים

עקרון ההסכמה

23. בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות"), כדי שאיסוף מידע אישי יהיה חוקי **יש לקבל את הסכמת נושא המידע לכך** או להצביע על מקור חוקי אחר המאפשר למוסד האקדמי לעשות כן. ככל שלא קיים מקור חוקי אחר, ניתן להשתמש באמצעים טכנולוגיים לשמירה על טוהר הבחינה אך ורק בהסתמך על הסכמתו של הנבחן לשימוש בהם.
24. כדי שההסכמה תהיה תקפה עליה להיות הסכמה חופשית ומדעת. בשל פערי הכוחות בין הנבחן למוסד האקדמי, משמעות הדבר היא כי על המוסד לאפשר לנבחן לסרב להיבחן במתכונת של בחינה מרחוק שנעשה בה שימוש באמצעים לשמירה על טוהר הבחינה, מבלי שהסירוב יהיה כרוך בפגיעה בזכויותיו, וזאת גם אם המוסד בחר להשתמש באמצעים אלה לאחר שקבע כי השימוש בהם מידתי. לפיכך, כאשר מתקבלת החלטה על שימוש באמצעים טכנולוגיים לשמירה על טוהר הבחינה, על המוסד האקדמי לאפשר לנבחן חלופות אחרות, במידת האפשר ובכפוף גם למגבלות המוטלות בעטיו של משבר הקורונה, ומכל מקום להבטיח כי הסירוב לא יפגע בזכויותיו של הנבחן או בהערכתו האקדמית. דחיית מועד הבחינה עד למועד שבו ניתן יהיה לקיימה באופן פרונטלי תחשב חלופה יעילה, גם אם הדבר כרוך בשינוי תכנית הלימודים של אותו סטודנט, ובלבד שלא שייגבה בעטיה שכר לימוד נוסף.

PPA@justice.gov.il | 02-6467064 | 073-3928555
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

<u>חובת הגילוי</u>

25. על המוסד האקדמי להתריע בפני הנבחן, מראש, על כוונתו לעשות שימוש באמצעים טכנולוגיים לשמירה על טוהר הבחינה.[5] במסגרת זו, מומלץ כי מועד הפנייה לקבלת הסכמת הנבחן יהיה מוקדם ככל הניתן, באופן שיאפשר לו לסרב להיבחן במתכונת האמורה, אם יחפוץ בכך, מבלי שייפגע. כמו כן, יש ליידע את הנבחן בדבר החלופות העומדות בפניו במקרה שבו סירב להיבחן במתכונת זו. ניתן לקבל **הסכמה עקרונית** לשימוש באמצעים לשמירה על טוהר הבחינות מרחוק ואין צורך לקבל הסכמה נפרדת לכל בחינה, אך במקרה זה יש להבהיר במפורש באילו קורסים תתקיים הבחינה במתכונת זו, מהי רמת הפיקוח בכל בחינה ומהי החלופה למתכונת הבחינה.

26. **הסכמת הנבחן תהיה תקפה רק לאחר שהמוסד האקדמי עמד בחובת הגילוי**.

27. יש לאפשר לנבחן לחזור בו מהסכמתו, במועד סביר בנסיבות העניין, מבלי שהדבר יהיה כרוך בפגיעה בזכויותיו. חזרה מהסכמה אין משמעה ביטול התוקף של בחינות אשר התקיימו לפני שהנבחן חזר בו מהסכמתו, וזו תהא תקפה רק ביחס לבחינות עתידיות.

28. כאשר מתבקשת הסכמתו של הנבחן, יש להסביר לו מהי מתכונת הבחינה, מהם אמצעי השמירה על טוהר הבחינה, איזה מידע ייאסף (כגון צילום מסך, הקלטת מהלך הבחינה וכיו"ב), מהי מטרת איסוף המידע ומה ייעשה במידע, זכותו לסרב למתכונת הבחינה והחלופות לבחינה, משך הזמן שבו יישמר המידע, העברת המידע לצד שלישי אם מתוכננת כזו. בנוסף, מומלץ ליידע את הנבחן בדבר זכותו לעיין במידע אודותיו, ולבקש את תיקון המידע או את מחיקתו בנסיבות הקבועות בחוק.[6]

29. ככל שנשקל השימוש באמצעים טכנולוגיים לשמירת טוהר הבחינה המתבססים על תהליך קבלת החלטות אוטומטי, כגון אמצעי ניטור העתקות שלא באמצעות התערבות אנושית (השוואת תשובות אוטומטיות לניטור העתקות; ניטור התנהגויות מוגדרות מראש כגון הסטת מבט ועוד), מומלץ להסביר לנבחן ולפרט כיצד מנוטרת התנהגות הפוגעת בטוהר הבחינה ואיזה סוג של התנהגות המערכת מנטרת. ככל שהוחלט לפסול בחינה יש להסביר מה היה המידע אשר גרם למערכת לפסול את הבחינה. מומלץ שהקביעה הסופית בדבר קיומה של התנהגות הפוגעת בטוהר הבחינה תעשה בידי בוחן אנושי.

30. בשל איסוף המידע הרב על ידי אמצעים לשמירה על טוהר הבחינה, מומלץ לנסח מדיניות פרטיות לבחינות במתכונת זו, אשר תהיה נפרדת ממדיניות הפרטיות הכללית של המוסד האקדמי, ובה להתייחס גם לפריטי המידע הנאסף, מה ייעשה במידע וכמה זמן יישמר. מדיניות הפרטיות תתעדכן מעת לעת ותכלול התייחסות לעדכונים במערכת הטכנולוגית המשמשת לשמירה על טוהר הבחינה, ככל שיבוצעו עדכונים כאמור.

[5] ראו סעיף 11 לחוק הגנת הפרטיות.
[6] ראו סעיפים 13-14 לחוק הגנת הפרטיות.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

דגשים נוספים

31. **חוק הגנת הפרטיות, התקנות אשר הותקנו מכוחו והנחיות הרשות להגנת הפרטיות כוללים הוראות רלבנטיות נוספות, אשר יישומם כראוי יפחית את הפגיעה בפרטיות הנבחנים במתכונת המתוארת במסמך זה וימזער את החשש להתנהלות לא מידתית של המוסד האקדמי.**

<u>מימוש זכותו של הנבחן לעיין במידע</u>

32. סעיף 13 לחוק, והנחיות הרשות להגנת הפרטיות,[7] קובעים כי לנושא המידע ישנה זכות לעיין במידע על אודותיו, על פי בקשתו. בנוסף, סעיף 14 לחוק מקנה לנושא המידע זכות לתקן מידע שגוי או בלתי מעודכן אודותיו ולבקש למחקו.

33. במקרה של בחינות מרחוק, **זכות העיון חלה על כל המידע הקשור לבחינה לרבות המידע אשר נמסר לצרכי הזדהות, צילומי וידאו, וכן על תשובות הנבחן לבחינה. מומלץ כי זכות העיון תמומש באמצעות ממשקים מקוונים, או באמצעות העברת קובץ דיגיטלי.** ככל שבהקלטה מופיעים נבחנים נוספים, מוצע לפעול לפי החלופות המנויות בסעיף 3.1.5.4 להנחיית רשם מאגרי המידע 4/2012.[8]

<u>משך שמירת המידע</u>

34. שימוש במידע או בידיעה על ענייניו הפרטיים של אדם, ובכלל זה עצם שמירת המידע, כאשר אינו נחוץ עוד למטרה לשמה נמסר או למטרת המאגר, מהווה הפרה של עקרון צמידות המטרה הקבוע בסעיפים 2(9) ו-8(ב) לחוק הגנת הפרטיות, ויוצרת סיכוני אבטחת מידע מיותרים, ומשום כך גם מהווה פגיעה בפרטיות ומפרה את הוראות חוק הגנת הפרטיות.[9]

35. לפיכך, מומלץ למחוק את המידע במועד שבו המידע מפסיק לשרת את המטרה לשמה נאסף, ואין לעשות בו שימוש מעבר למטרה אשר לשמה נאסף המידע (קרי, הזדהות ושמירה על טוהר הבחינה), כפי שהוגדרה במדיניות הפרטיות.

36. התשובה לשאלה מהו המועד שבו המידע מפסיק לשרת את המטרה לשמה נאסף, נגזרת ממהות המידע. למשל, מידע אשר נועד לאמת את זהות הנבחן (כגון צילום תעודת זהות) הופך ככלל בלתי רלבנטי עם סיום תהליך ההזדהות. מידע אשר נאסף כדי להבטיח את טוהר הבחינה המקוונת, כגון צילומי וידאו, יהפוך לכאורה בלתי רלבנטי כאשר אין טענת העתקה או מרמה.

---

[7] הנחיית רשם מאגרי המידע 1/2017 " תחולת הוראות חוק הגנת הפרטיות על זכות העיון בהקלטות קול, וידאו ומידע דיגיטלי נוסף". זמינה ב: https://www.gov.il/BlobFolder/policy/right_of_access/he/video.pdf.

[8] הנחיית רשם מאגרי המידע 4/2012 "שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן". זמינה כאן: https://www.gov.il/BlobFolder/policy/surveillance_cameras_guidelines/he/The%20use%20of%20security%20cameras.pdf.

[9] ראו גם תקנה 2(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, המטילה על בעל המאגר חובה עתית לבחון האם המידע שהוא שומר אינו רב מן הנדרש למטרות המאגר.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

37. נדגיש כי איסוף מידע רב ושמירתו מייצרים סיכוני אבטחת מידע, ולכן מדובר גם באינטרס של המוסד האקדמי למזער את כמויות המידע אודות הסטודנטים למינימום ההכרחי, ובכך למזער את החשיפה לאירועי אבטחת מידע אפשריים. לצורך כך מומלץ כי המוסד האקדמי יקבע מדיניות ברורה בנושא משך הזמן שבמהלכו יישמר המידע, על סוגיו השונים, וישקף זאת גם במדיניות הפרטיות שתפורסם כחלק מהתהליך של קיום בחינות מקוונות מרחוק.

<u>מיקור חוץ</u>

38. ברוב המקרים מערכות לקיום בחינות מקוונות מרחוק מסופקות למוסד האקדמי ע"י ספקי שירותים ומערכות במיקור חוץ. על המוסד האקדמי לוודא כי הגורמים עימם הוא מתקשר לצורך קיום בחינות מקוונות הינו בעל מומחיות, ניסיון, תשומות ומשאבים מתאימים ורלבנטיים להגן על פרטיות הנבחנים ולאבטח את המידע. בשל כמות המידע האישי ורגישותו, יש להקפיד על בחינת אמינות ספקי השירותים עימם מתקשר המוסד האקדמי לצורך קיום בחינות מקוונות.
39. ההסכם בין המוסד האקדמי לבין נותן השירותים יכלול הוראות בדבר אבטחת מידע אצל ספק שירותי החוץ ובדבר חובתו לאפשר ביצוע ביקורות עצמאיות של המוסד האקדמי. ההסכם יכלול הוראה מפורשת לפיה הטיפול במידע יעשה לפי הוראות המוסד האקדמי, וכן יגדיר מה הם השימושים המותרים במידע. מומלץ כי ההסכם יכלול מגבלה וסנקציות על שימושים נוספים.
40. לפני ההחלטה האם לעשות שימוש בטכנולוגיות לשמירה על טוהר הבחינה ובאיזו טכנולוגיה לבחור, וכן לפני התקשרות במיקור חוץ מומלץ לערוך תסקיר השפעה על פרטיות, אשר יתייחס גם להיבטים של מיקור חוץ.
41. בכל הנוגע להיבטי אבטחת מידע בעת התקשרות עם גורם חיצוני, ראו החובות המוטלות בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "תקנות אבטחת מידע"). להרחבה לגבי ההסדרים הרלבנטיים למיקור חוץ ראו הנחיית הרשות להגנת הפרטיות מס' 2/2011 "שימוש בשירותי מיקור חוץ לעיבוד מידע אישי".[10]
42. בעת העברת מידע אישי על אודות סטודנטים לספק שירותי מיקור חוץ, יש להקפיד על הגבלת אפשרות הגישה למידע לעובדים אשר גישה כאמור חיונית לביצוע תפקידם, ויש להקפיד על מחיקת כל המידע שברשות הספק לא יאוחר מהמועד בו המידע אינו נחוץ עוד למטרה לשמה נמסר או למטרת המאגר.

[10] זמין ב: https://www.gov.il/he/departments/policies/outsourcing.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

<u>אבטחת מידע אישי והכנת תסקיר השפעה על פרטיות</u>

43. מידע יכול לדלוף בשל שורה של גורמים לרבות אי סגירת פונקציית שיתוף המסך בתום הבחינה, שיתוף לא רצוני של פרטים אישיים הנמצאים בחדרו של הנבחן, גניבת זהות של הנבחן ע"י מורשי גישה או ע"י מי שאינו מורשה לגשת למידע, גניבת קבצי הווידאו אודות הנבחנים, הן בשלב הבחינה והן בשלב ההזדהות ועוד. על כן, יש להקפיד על איסוף מידע למינימום הנדרש לצורך השמירה על טוהר הבחינה ואין לאסוף מידע אשר אינו נחוץ לצורך זה. בהקשר זה מומלץ להציע לנבחן, לפני הפעלת צילומי הווידאו, להסיר מהחדר בו הוא שוהה בעת הבחינה, סממנים אישיים שיש בהם משום פגיעה בפרטיותו. בנוסף, המוסד האקדמי ימפה את כל סוגי המידע האישי הנאספים ומעובדים בבחינות מרחוק ויוודא הכרחיות כל אחד מהם לצורך קיום הבחינה ושמירה על טהרתה.

44. סעיף 17 לחוק הגנת הפרטיות קובע כי בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז -2017 קובעות את האופן שבו יש לאבטח את המידע. **על המוסד האקדמי לוודא כי הן המוסד האקדמי והן הגורמים עמם הוא מתקשר, עומדים בנהלי אבטחת מידע במלואם בהתאם לנדרש בתקנה 4 לתקנות אלו**, ויש לבחון את תוקפם של נהלים אלה מעת לעת בהתאם להוראות התקנות.

45. כמו כן, מומלץ כי המוסדות האקדמיים יבצעו הליך שיטתי ומושכל של בחינת מלוא הנסיבות וההיבטים של הגנת הפרטיות הכרוכים בבחינות מרחוק, כגון באמצעות תסקיר השפעה על פרטיות של המערכת הטכנולוגית לבחינה מרחוק, בכדי לזהות, למפות ולהפחית סיכונים לפרטיות הנבחנים. לשם כך ניתן להיעזר במדריך בעניין תסקיר השפעה על פרטיות אשר פורסם על ידי הרשות להגנת הפרטיות.[11]

46. התסקיר יתייחס לכל אמצעי טכנולוגי אשר שולב במערכת ונועד לשמור על טוהר הבחינה; סיכונים למידע משך כל זמן המחזור של המידע, לרבות תהליך ההזדהות, התחברות המערכות הטכנולוגיות לציוד הקצה של הנבחן (שיתוף מסך, מצלמות), חדירה למחשב הנבחן, אחסון המידע, עיבוד המידע, ומחיקתו. התסקיר יפרט מה הם האמצעים הרלבנטיים להסרה או הפחתה של כל סיכון לפרטיות (סיכוני אבטחת מידע ואחרים) אשר נכלל בו.

47. מבלי לגרוע מכלל ההוראות המחייבות של תקנות אבטחת מידע, נדגיש כי יש לוודא קיומה של תכנית עבודה שנתית העומדת בדרישות התקנות, ולקיים ביקורת תקופתית, פנימית או חיצונית.

[11] להרחבה על אופן עריכת תסקיר השפעה על פרטיות ראו המדריך שפרסמה הרשות להגנת הפרטיות בנושא: https://www.gov.il/blobFolder/generalpage/privacy_by_design/he/privacyimapctassessment2015.pdf.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

48. בנוסף, יש להקפיד על הרשאות גישה למאגר באופן שבו גישה תתאפשר רק עבור מי שנדרש לכך לצורך ביצוע תפקידו,[12] וביטול הרשאות גישה של מי שסיים תפקידו, ויש להתקין אמצעי הגנה מתאימים מפני חדירה לא מורשית בכל אותן נקודות במערכת הפתוחות לרשת האינטרנט. בנוסף, כדי להגן על המידע יש להטמיע אמצעי אנונימיזציה והצפנה ככל שניתן.
49. יש לנסח מדיניות לצמצום אפשרות קרות אירועי אבטחת מידע ולהתמודדות עמם ככל שהתרחשו.
50. יש לתעד פניות בנושא פרטיות ואבטחת מידע בכדי להתמודד עם כשלים אפשריים.
51. יש להבטיח עמידות, סודיות, בטיחות וזמינות של המערכות הטכנולוגיות הרלבנטיות לבחינות מקוונות.
52. יש לבצע בדיקות תקופתיות לאמצעי אבטחת המידע.
53. יש להבטיח כי כל בעלי זכות הגישה למידע יטפלו במידע לפי הנחיות והוראות בעל מאגר המידע, קרי, המוסד האקדמי.
54. מומלץ לקיים הדרכות תקופתיות בנושא שמירה על פרטיות ואבטחת מידע עבור מורשי הגישה למידע אישי במערכות בחינות מקוונות.
55. מומלץ לתעד פעולות עיבוד מידע לרבות מיפוי נושאי מידע, קטגוריות המידע המעובד, וצדדים שלישיים המקבלים את המידע או גישה אליו, משך הזמן בו נשמר המידע ואמצעי אבטחת מידע אשר הוטמעו במערכות.

<u>העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה</u>

56. במקרים רבים, בעת שימוש באמצעים דיגיטליים, מידע מועבר אל מחוץ לגבולות המדינה לצרכי תפעול ואחסון. כך למשל, שמירת הקלטת בחינה מרחוק, יכולה להיעשות הן על המחשב האישי, והן בחוות שרתים (ענן) הנמצאת במדינה זרה.
57. העברות מידע מחוץ למדינה כפופות לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.
58. בשל פערי דינים בין מדינות, ובשל העובדה שיש מדינות בהן ההגנה על הפרטיות אינה מספקת, מומלץ למעט ככל הניתן מהעברות מידע אל מחוץ לגבולות המדינה.
59. בשל פערי הכוחות בין מוסדות להשכלה גבוהה ובין הסטודנטים, ככל שאין מנוס מהעברת מידע אל מחוץ למדינה מומלץ שלא להעביר מידע לגורם הפועל במדינה בה רמת ההגנה על המידע פחותה מזו הקבועה בדין הישראלי, גם אם הנבחנים נתנו הסכמתם לכך.

[12] לדוגמה מפקח, מרצה, ועדת בוחנים וכיו"ב.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

<u>סיכום</u>

התקופה הנוכחית מציבה אתגרים רבים למוסדות להשכלה גבוהה ולסטודנטים המבקשים להמשיך ולקיים לימודים בתקופה של סגרים וריחוק חברתי. מובן הצורך במציאת פתרונות יצירתיים ללימודים מרחוק ולקיום בחינות באופן שאינו פרונטלי, וזאת תוך שמירה על טוהר הבחינה, לשם קיום רמה אקדמית נאותה ושמירת עקרון החופש האקדמי.

עם זאת לאמצעים טכנולוגיים לשמירה על טוהר הבחינה ישנה השפעה ניכרת על פרטיות הסטודנטים, ועל כן יש להקפיד וליישם את ההוראות וההנחיות שבמסמך זה ובדין הכללי, בכדי להגן על המידע האישי של הסטודנטים ועל פרטיותם.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב