BDO

PrivacyOps Forum

מי אמר GDPR?

פסוקו של יום בפרשנות פרטית

כתב: גלעד ירון
ערכה: סיון מנחם

קצת על עצמי ומה כל זה?

שלום.

כבר למעלה מ-30 שנה אני מתגלגל בעולם ניהול מערכות המידע, תכנון פתרונות וייעוץ בתחום הגנת הסייבר והגנת הפרטיות.

לאחר שנדבקתי בווירוס הפרטיות (זה די מסוכן!) הקמתי את חטיבת הגנת המידע והפרטיות של פירמת הייעוץ הבינלאומית BDO.

הצוות הישראלי עובד בשיתוף פעולה הדוק עם 600 מומחי פרטיות של הפירמה מרחבי העולם, המביאים עמם ידע וניסיון הקשור לחוקים והתקנות המקובלים בארצותיהם.

אנחנו מדברים עם כולם - מנכ"לים, יועצים משפטיים, מנהלי סיכונים, מנהלי מחשוב ואבטחת מידע, ומנסים לסייע להם להתמודד עם החוקים הסבוכים האלה, הסטנדרטים הארוכים ודרישות הלקוחות שלא נגמרות לעולם.

אנחנו עוזרים להם להבין מה רוצים מהם, לתרגם את זה לשפה אנושית ולתוכניות עבודה פרקטיות, כך שהם יוכלו לעמוד בדרישות מבלי לפגוע במשימותיהם העסקיות.

אני מאמין בחשיבות נושא הגנת המידע ופרטיות בישראל ומנסה לתרום לקידומו.

אני מפרסם כתבות ומאמרים בנושא הפרטיות כמעט מידי יום.

אתם מוזמנים לעקוב:

הפרופיל שלי ב- LinkedIn:
https://www.linkedin.com/in/giladyaron/.

ערוץ לינקדאין "פרטיות שקטה" בו אני מפרסם תובנות בנושא הגנת הפרטיות אליו ניתן להצטרף בקישור הבא:
https://chat.whatsapp.com/JLBJDkfZ7k5FCUGBBjsofS

99 יום לפני פרוץ ה- GDPR פרסמתי יום יום פרשנות אישית, בלתי מחייבת, של חוק הפרטיות האירופאי, פסוק פסוק. איני מתיימר להיות עורך דין או משפטן, אין לכתוב תוקף משפטי. יחד עם זאת - אם הכתוב יעזור למישהו להבין טיפה יותר את ה- GDPR, דיינו.

החוברת מסודרת על פי סדר הפסוקים ב"יצירה" המקורית.

קריאה מהנה!

גלעד ירון
דירקטור
ראש חטיבת הגנת המידע והפרטיות
GiladY@bdo.co.il
052-6755514

הוראות כלליות

1 | יוצאים לדרך

בפסוק הראשון של הפואמה מציג המשורר את הגיבורים הראשיים - אנחנו.

להפתעתנו אנו מגלים כי המספר הכל יכול מאמין כי המידע אודותינו, האנשים הטבעיים, שייך לנו (אם אנחנו תושבי אירופה... אם לא - קראו ספר אחר ...).

החוק מיועד להגן על זכויותינו ובפרט על הצורך להגן על המידע הפרטי שלנו.

מה זה מידע פרטי? שאלה טובה, על כך יסופר בפסוקים הבאים.

2 | תגידו אבל, על מה החוק חל?

פסוק שני ובו מסופר, על מה חל חוק ה - GDPR המובר. הסופר מסביר כאן את התמונה המרכזית בה עוסקת היצירה.

מדובר על עיבוד, ממוחשב או ידני, של מידע פרטי של אנשים בני תמותה (אך לא אלו שכבר אינם אתנו) במטרה לייצר אוסף של רשומות (Filing system).

זה נשמע כמו מושג ממדריך בסיסי למשתמש במחשב, לא מיני ולא מקצתי. מדובר על אוסף רשומות בכל צורה וצבע, ללא קשר לאופן המימוש הטכנולוגי שלו.

הסופר ממהר ומסביר כי הוא אינו עוסק כלל ועיקר במידע אשר מקורו אינו באיחוד האירופי (שימו לב - מדובר על המקור, לא על המקום בו הוא שמור).

כך גם מידע שמעובד על ידי פרטים, ולא ארגונים, הוא לא חלק מהסיפור הזה.

3 | מה לנו ולאירופה

עד כה הציג לנו המספר את גיבורי הסיפור, תושבי אירופה, ואת נושא הסיפור - הגנה על פרטיותם.

הפסוק שלנו היום עוסק בזירת העלילה, התשובה לכאורה פשוטה - אירופה.

בפועל זה קצת יותר מורכב: כל ארגון ברחבי העולם העוסק במידע פרטי של תושבי אירופה נוטל חלק בסיפורנו.

כדי שלא יהיה לנו ספק למה התכוון המשורר, הוא מסביר כי מדובר על ארגונים המציעים סחורות ושירותים לתושבי אירופה ללא קשר למקום ואופן התשלום ואפילו כאשר השירות אינו כרוך בתשלום. בנוסף הוא מתייחס לארגונים המנטרים את התנהגותם של אנשים השוהים באירופה. בפרט, מדובר על בניית פרופיל התנהגותי ממוחשב וקבלת החלטות על בסיס פרופיל זה.

בפרשנות שמעניק הסופר הוא מרחיב ונותן דוגמאות כיצד ניתן לזהות ארגון הסוחר עם אירופה. כך, למשל, אתר אינטרנט הכתוב בשפה אירופית כמו צרפתית מן הסתם פונה לקהל אירופאי.

4 | הגדרות וצרות אחרות

פסוק זה מורכב כולו מהגדרות שישמשו אותנו בהמשך הדרך, יש כאן 26 הגדרות. אנו נסקור אך ורק שתיים מהן - מידע פרטי ומערכת תיוק. על כל ההגדרות האחרות נדון במסגרת הפסוקים הרלוונטיים להן.

בספרנו, מידע פרטי מוגדר כמידע אותו ניתן לקשר, באופן ישיר או עקיף, לאדם פרטי, כגון שם, תעודת זהות, פרטי מיקום והזהות הדיגיטלית שלו או למאפיין אחד או יותר הקשורים לתכונות הפיזיות, פיזיולוגיות, נפשיות, כלכליות או תרבותיות של אדם פרטי.

שימו לב שזו הגדרה רחבה מאוד. יחד עם זאת, אל תיסחפו יתר על המידה. היזהרו לא לטבוע. לא כל IP באשר הוא מהווה מידע פרטי.

נחזור לעיין במה שלמדנו לפני יומיים כאשר דנו **בפסוק 2** שעסק בתחולת החוק. שם הסביר לנו הסופר כי החוק עוסק במידע הנמצא ב"מערכות תיוק".

בפסוק זה מסבירים לנו כי מערכת תיוק מתייחסת לכל מידע פרטי המאורגן באופן שיטתי ואליו ניתן לגשת על פי קריטריון מסוים. לצורך המחשה, תיקיה פיזית של מועמדים המסודרת על פי א-ב עונה להגדרה זו.

עקרונות

5 | שמרו על העקרונות שלכם

פרק זה מציג לנו לראשונה את עקרונות הרגולציה המפורטים בפסוקים 5-11.

פסוק 5 מגדיר את עקרונות היסוד שחלקם מורחבים בפסוקים הבאים.

יעלו ויבואו ששת עקרונות היסוד, ראשון ראשון ואחרון אחרון:

1. יש לעבד את המידע הפרטי בהתאם לחוק, באופן הוגן, תוך שמירה על שקיפות
2. יש להגדיר היטב את המידע שנאסף, מטרות האיסוף והעיבוד
3. יש לבצע אך ורק את העיבוד שהוגדר ולאסוף אך ורק את המידע ההכרחי לשם כך
4. יש להקפיד על דיוק ועדכניות המידע
5. יש לשמור את המידע לפרק הזמן המינימלי ההכרחי ליעדים שהוגדרו
6. יש להגן על המידע מאובדן, פגיעה או שיבוש על מנת לשמור על שלמותו וסודיותו

6 | ומה אם ביום שלישי לא בא לי להסכים?

סעיף 6 של הרגולציה דן בתנאים המשפטיים המתירים לאסוף ולעבד מידע פרטי של תושבי אירופה. אם אף אחד מן התנאים לא תקף, תעשו לעצמכם טובה ואל תעשו זאת.

והזוכים הם:

1. הסכמה מפורשת, ברורה ומתועדת של נשוא המידע לעשות בו שימוש ספציפי
2. המידע נדרש כחלק מחוזה בו נשוא המידע נוטל חלק
3. המידע נדרש על פי דין במדינה בה נמצא מעבד המידע
4. המידע נדרש על מנת להגן על אינטרס חיוני של נשוא המידע
5. המידע נדרש כדי לשמור על האינטרס הציבורי

כל זאת על קצה המזלג. הכתוב מפרט, מכיל הסברים רבים ומפרשן את עצמו ברסיטלים והערות לרוב. יחד עם זאת הוא משאיר המון עבודה לעורכי הדין להגות בה יומם ולילה.

7 | איך מסיקים שאתה באמת מסכים?

בפסוק הקודם בספרנו למדנו כי אם אין לנו תירוץ ממש ממש, התנאי היחיד המתיר לנו לשמור ולעבד מידע פרטי הוא הסכמתו של נשוא המידע.

פסוק 7 של היצירה מוקדש כולו לשאלה "כשאתה אומר כן למה אתה מתכוון".

"כדי שנהיה בטוחים בכל מאת האחוזים שאתה באמת מסכים אתנו:

1. להחזיק ראיות לכך שאכן קיבלנו הסכמה
2. להציג לנשוא המידע את הבקשה להסכמה בצורה ברורה וקריאה. "נא לאשר את ה-Cookies" זו לא שפה של אדם טבעי
3. לאפשר לנשוא המידע לשנות את דעתו ולהסיר את ההסכמה בכל רגע נתון
4. לוודא כי אנו דורשים הסכמה אך ורק בהקשר למידע הרלוונטי לתהליך

8 | ילד אסור, ילד מותר

ילדים ראויים להגנה מיוחדת על פרטיותם שכן הם אינם בהכרח מבינים עד הסוף את הסיכונים וההשלכות הנגררות מחשיפת פרטיותם.

בשל כך מקדיש המחוקק חשיבה מיוחדת לפרטיות המידע שלהם.

רק אתמול דיברנו על התנאים לוודא כי ההסכמה לשמור ולעבד מידע פרטי הינה ראויה.

פסוק שמיני של היצירה מוסיף תנאי נוסף: במידה ומדובר על ילד מתחת לגיל 16, ההסכמה תהיה מקובלת רק אם ניתנה על ידי הוריו של הקטין.

9 | להיות יחיד ומיוחד

הפסוק שלנו עוסק במידע ששייך לקטגוריה שהסופר מכנה "קטגוריות מיוחדות". מדובר על נתונים אישיים החושפים מקור גזעי או אתני, דעות פוליטיות, אמונות דתיות או פילוסופיות, או חברות באיחוד המקצועי, ועיבוד נתונים גנטיים, נתונים ביומטריים לצורך זיהוי ייחודי של אדם טבעי, נתונים הנוגעים לבריאות או נתונים הנוגעים לטבע טבעי. חיי המין של האדם או נטייתו המינית.

בעיקרון הוא אוסר על עיבוד של מידע כזה כלל וכלל למעט בהסתייגויות הבאות:

נושא הנתונים נתן הסכמה מפורשת לעיבודם של נתונים אישיים למטרות מוגדרות אחת או יותר

- העיבוד נחוץ לצורך נדרש על פי חוק בהתאם לדיני התעסוקה והביטחון הסוציאלי וההגנה הסוציאלית,
- העיבוד מתבצע במהלך פעילותו הלגיטימית תוך הגנה נאותה על ידי קרן, עמותה או כל גוף אחר שלא למטרות רווח שמטרת העיבוד מתייחס לנתונים אישיים שפורסמו באופן מפורש על ידי הנבדק;

  עיבוד הכרחי לצורך ביסוס, מימוש או הגנה של תביעות משפטיות;

  העיבוד נחוץ מסיבות בעלות אינטרס ציבורי מהותי, על בסיס חוק האיחוד או מדינת החבר שיהיה ביחס למטרה הנשקפת, לכבד את מהות הזכות להגנת נתונים ולקבוע צעדים מתאימים וספציפיים לשמירה על זכויות היסוד והאינטרסים של הנבדק;

  העיבוד נחוץ למטרות רפואה מונעת או תעסוקתית.

- העיבוד נחוץ מטעמי אינטרס ציבורי בתחום בריאות הציבור.

10 | רישום פלילי? עניין שלי!

רישומים פליליים עלולים להטיל על האדם כתם לכל החיים.

המחוקק האירופאי רואה לנכון להקדיש סעיף מיוחד לנושא זה, הוא מנחה באופן חד משמעי כי רישומים מסוג זה יכולים להישמר אך ורק על ידי רשויות רשמיות שהוסמכו לכך.

11 | אני סובב לי במעגל

פסוק זה של הרגולציה עוסק בבעיה מעגלית. איך נוכל לדאוג לזכויות הפרט אם לא יהיו לנו פרטים המזהים אותו?

אבל רגע, אם אין לנו פרטים מזהים של האדם ואיננו יכולים לקשר את המידע שבידינו לאדם מסוים הרי שעל פי ההגדרה אין לנו מידע פרטי. הכותב החכם מוציא אותנו מהמלכוד ופותר אותנו מהצורך לאסוף פרטים מיותרים רק כדי לשמור עליהם.

מה למדנו מזה? שלא תמיד כל המרבה הרי זה משובח. אל תחפשו בעיות במקום שאינן קיימות.

זכויות נושאי המידע

12 | אין מאוחר ומוקדם בשקיפות

נראה שבפסוק 12 של היצירה העורך קצת התרשל (בכל אשמה ההפקה?) והוא מתייחס לפסוקים 13, 14, 15, 22 ו-34 לפני שקראנו אותם, משל אין מאוחר ומוקדם ביצירה. הפסוק עוסק בשקיפות יש להקפיד על שקיפות מלאה לנשוא המידע בכל מה שקשור לאיסוף המידע, עיבודו, היכולת לגשת אליו, לעדכנו ואף למחוק אותו.

שיתוף המידע צריך להיעשות:

1. באופן ברור, מדויק ובאופן שיהיה קל לגשת אליו, יש לספק מידע זה בכתב או באופן אלקטרוני
2. ניתן לספק את המידע לנשוא המידע בעל-פה, כל עוד הבטחנו שאכן האדם שעמו אנו מדברים הוא הוא ולא אחר
3. אין לסרב לבקשה למידע אלא עם כן לא קבלנו הוכחה ודאית שההוא הוא ההוא

13 | אז.... גידי לא, תגידו לו

כאשר נאספים נתונים אישיים הישר מבעל המידע, יש לספר לו את כל הדברים הבאים:

- זהות ופרטי יצירת הקשר של הבקר, ובמידת הצורך, של נציג הבקר;
- פרטי הקשר של קצין הגנת המידע;
- מטרות העיבוד שלשמן מיועדים הנתונים האישיים וכן הבסיס החוקי לעיבוד;
- הנמענים או הקטגוריות של מקבלי הנתונים האישיים;
- האם ואיך יועברו נתונים אישיים למדינה שלישית או לארגון בינלאומי;
- התקופה בה מאוחסנים הנתונים האישיים, או אם הדבר אינו אפשרי, הקריטריונים המשמשים לקביעת תקופה זו;
- קיום הזכות לבקש מהבקר גישה לתיקון או מחיקה של נתונים אישיים או הגבלת עיבוד הנוגעת לנבדק או להתנגד לעיבוד וכן הזכות לניידות נתונים;
- הזכות למשוך את ההסכמה בכל עת, מבלי לפגוע בחוקיות העיבוד על סמך הסכמה;
- הזכות להגיש תלונה ברשות מפקחת;
- האם מסירת נתונים אישיים הינה דרישה סטטוטורית או חוזית, או דרישה הכרחית להתקשרות בחוזה, וכן האם נושא הנתונים מחויב למסור את הנתונים האישיים וההשלכות האפשריות של אי מסירת נתונים כאמור;
- אם קיים תהליך של קבלת החלטות אוטומטית (פרופיילינג) ומה הלוגיקה שעומדת מאחוריו.

14 | אל נא תגיד עבשיו אין לי פנאי, ספר לי סיפור עלי

הפסוק נראה לנו מאוד מובן. הוא מדבר על מה צריך למסור לנשוא המידע: למה, כמה ואיך אנחנו מטפלים במידע שלו. חדי העין יבחינו בוודאי שעל כך בדיוק דנו בפסוק הקודם.

אותם תשעה תנאים חוזרים על עצמם מילה במילה. האם בוחנים את רמת ההקשבה שלנו? גם, אבל לא רק. הפעם מדובר על מידע שאספנו ממקורות אחרים ולא ישירות מנשוא המידע.

יחד עם זאת, למיטיבי הלכת שצלחו את אותו הטקסט המופלא שוב, מחכה הפתעה בסוף הדרך. במידה וקשה המסע ויידוע כל אחד מנשואי המידע צר וכבד לכם, כמו למשל, מידע רב הנאסף במחקר, אז מספיק שתשמרו טוב טוב על המידע.

הגדרה קצת לא ממש מהודקת? גם המבקר הספרותי שלכם סבור כך. נראה שהכותב משאיר קצת מקום לפרנסתם של הפרשנים והמשפטנים בשנים הקרובות.

15 | הזכות לשאול הכול, ולקבל תשובה, מפורטת וטובה

פסוק 15 של היצירה אומר לנו דבר פשוט אבל חשוב ביותר: מותר וכדאי לשאול שאלות.

זכותנו לשאול כל מפעיל שירות: האם אתה שומר מידע עלינו? אם כן אז איזה, ומה יוצא לנו מזה?

דרשו פרטים מדויקים: מה עושים עם הנתונים? למי הם חשופים? למי אתה שולח אותם? כמה זמן הם נשמרים? איך אתה מגן עליהם כך שיגיעו רק לגורמים הנכונים?

זה יותר מסתם פסוק מרגולציה יבשה. תמיד, בכל מצב, יש לנו זכות לשאול, הכול, בקול גדול ואם התשובה מבהירה לנו כי זה לא מה שציפינו, ניתן לומר מילה קטנה - די!

16 | כמה הרבה זה הרבה?

במספר מקומות ביצירה נאמר שאם ישנו "מידע פרטי בקנה מידה נרחב" יש לנקוט בצעדים משמעותיים יותר להגנתו. למשל, מינוי בעל תפקיד קצין הפרטיות.

בניגוד לתקנות הישראליות, הקובעות קריטריונים ברורים וחד משמעיים לרמת ההגנה הנדרשת, החוק האירופאי אינו עונה לנו מי יודע כמה, מי יודע איך ולמה?

מועצת מנהלי הפרטיות של אירופה (שנקראה בעבר סעיף 29) נתנה בהם סימנים. הם מציעים לנו לתת את הדעת על השאלות הבאות:

- על כמה פרטים אנו מחזיקים מידע?
- מה נפח ההעברה ועיבוד המידע?
- מה משך עיבוד המידע וזמן שמירתו?
- מה רמת הפריסה הגיאוגרפית של המידע?

כל אלה פרמטרים שעוזרים לאבחן מידע נרחב. אבל מה? עדיין לא ברורים לנו מהם ערכי הסף של כל הפרמטרים הללו... חזרנו לנקודת ההתחלה . אז מה עושים?

לא מצאתי תשובת בספר לשאלה "כמה הרבה זה הרבה". לכן אני מציע:

- להפעיל שיקול דעת ולקבוע ספים הגיוניים;
- למצוא סימובין. התקנות הישראליות נראות לי כמו נקודת פתיחה טובה בהעדר הנחיות יותר ברורות מאחינו האירופאיים;
- כדאי לכלול את מאפייני המידע ברשומות עיבוד המידע (הרחבת פסוק 30 של החוק);
- חשוב לתעד היטב את השיקולים שלכם במסמכי המדיניות ובפרט במסמך קוד אוף קונדקט (עוד על כך בפסוק 40).

17 | הזכות להישכח, סתם כך, כי בא לי להיעלם

הגענו לפסוק העוסק בנושא משמעותי אך שנוי במחלוקת - הזכות להישכח.

פסוק זה מאפשר לנו לדרוש מחיקה של הפרטים שלנו גם אם הם נכונים! על הספק למחוק את המידע ללא שיהוי אם, בין היתר :

- המידע אינו נדרש יותר
- נשוא המידע מסיר את הסכמתו
- עיבוד המידע לא מסתמך על בסיס משפטי לגיטימי
- נדרש למחוק את המידע על פי דרישות חוק

אין צורך למחוק את המידע אם, בין היתר:

- הדבר פוגע בחופש הביטוי (ביטוי קטן טעון ומורכב מאוד...)
- יש לשמור את המידע אם קיימת דרישה חוקית או חוזית לבצע זאת.
- המידע תורם לאינטרס הציבורי (שוב - אבחנה לא פשוטה).

תקדים לנושא הינו פסק דין משנת 2014 בו הורה בית המשפט האירופאי להסיר מגוגל תוצאות חיפוש המעידות על כך שעורך דין ספרדי מסוים לא שילם את חובותיו לפני עשר שנים.

המתנגדים לזכות להישכח טוענים כי מחיקת ההיסטוריה תפגע בקבלת החלטות מושכלות. כך, למשל, יתכן כי העובדה שעורך דין זה הסתבך בחובות בעבר הופכת אותו פחות כשיר למלא את תפקידו היום.

על אחת כמה וכמה הדבר אמור לגבי אנשים אשר ביצעו פשעים חמורים יותר (מכירים את המנהג האמריקאי להציב שלטים בחצר המעידים כי כאן גר פושע מועד?)

18 | עצור! אתה מעבד את המידע שלי!
הזכות להתנגדות

בפסוק הקודם עסקנו בנשק יום הדין - היכולת של נשוא המידע לדרוש מחיקה של כל זכר מהנתונים שלו.

פסוק 18 מדבר על כלי קצת פחות קטלני - הזכות להגביל את העיבוד של המידע.

ניתן להשתמש בנשק זה בתנאים הבאים:

1. קיימים חילוקי דעות לגבי דיוק המידע
2. המידע אינו נאסף כחוק אך מעבד המידע דורש להגביל את השימוש בו ללא מחיקתו
3. המידע כבר אינו נדרש למעבד, אך הוא נדרש לנשוא המידע על מנת לבסס טיעון משפטי
4. נשוא המידע מתנגד לעיבוד של המידע והנושא נמצא בתהליך בירור

בתקופת ההגבלה אין לבצע כל עיבוד של המידע לבד מאחסונו אלא אם כן התקבל אישור מפורש של נשוא המידע לכך.

19 | כבר סיפרת לחברים של החברים שלך? חובת ההודעה

יתכן כי מידע שמסרת לספק מסוים אינו מסיים את דרכו אצל ספק זה אלא ממשיך ומתגלגל מספק לספק לספק.

גם אם הספק שלך נעתר לבקשתך להגביל או למחוק את המידע, יתכן כי המידע בכל זאת ממשיך לטייל לו ברחבי העולם.

פסוק 19 מנסה לעצור את המפולת, הוא דורש כי השולט במידע ידאג להודיע לכל אחד ואחד מאלה שקיבלו את המידע כי נשוא המידע ביקש להגביל או למחוק אותו.

המחבר מבהיר לנו כי יש לעשות זאת כל עוד הדבר אפשרי ואינו דורש "מאמץ בלתי מידתי".

מעניין..... מה זה "מאמץ בלתי מידתי"? לפרשנים והמשפטנים פתרונים.

20 | זכותי לדעת מה יודעים עלי - זה עניין של גישה

חוק הפרטיות האירופאי, GDPR, מקנה לכל אחד זכות לבקש ולקבל את המידע הפרטי שנשמר עליו אצל כל ספק שירות.

בנוסף על המידע, על המענה לכלול גם את הפרטים הבאים:

זכות דומה, אך מוגבלת יותר, קיימת גם בחוק הפרטיות שלנו: "כל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופוס, במידע שעליו המוחזק במאגר מידע."

החוקים אינם מפרטים כיצד מגישים את הבקשה. יונת דואר או כתובת אש בשמיים עשויות להיות דרכים לגיטימיות.

מומלץ להכין טפסים אלקטרוניים לבקשה, אבל, כאמור, כל דרך אחרת גם היא חוקית.

לימדו לזהות בקשות כאלה!

על התשובה להיות כתובה בצורה ברורה ומובנת כך שגם ילדים שיקבלו אותה יבינו מה כתוב בה.

אם קיבלתם בקשה כזו, אל תתפסו פאניקה.. וודאו מה בדיוק רוצים מכם והיערכו בהתאם.

הכינו מבעוד מועד נהלי עבודה לטיפול בנושא.

איך מוודאים שמי שמבקש את המידע הוא אכן מי שהוא טוען שהוא? שאלה חשובה פה, שם ובכל מקום. נדון עליה בפעם אחרת.

תהיו מוכנים לטפל בדרישות, ולא פחות חשוב, להוכיח שאתם אכן שומרי חוק למופת.

21 | טובת הציבור? תוביח, אחרת העיבוד אסור!

פסוק 18 עסק בתנאים בהם ניתן להתנגד לעיבוד מידע פרטי. לבקשת הקוראים, מרחיב הסופר את הדיון בנושא זה בפסוק 21 של היצירה.

השולט במידע עשוי לטעון כי המידע נדרש על מנת לשמור על האינטרס הציבורי או על ביטחון המדינה, אז הוא יכול.

לדרישת נשוא המידע יש לעצור את העיבוד כל עוד לא הוצג הבסיס החוקי הלגיטימי.

במקרה והמידע נדרש לטובת שיווק ישיר יכול נשוא המידע בכל עת לדרוש הפסקת העיבוד ובהתאמה יש להפסיק עיבוד זה באופן מידי.

יש לידע את נשוא המידע כי הזכויות הללו עומדות לרשותו.

22 | המחשב לא יחליט עלי

פסוק 22 מצהיר כי אין לקבל החלטות על בסיס עיבוד אוטומטי בלבד (פרופילינג).

כך, למשל, אין לסרב להעניק אשראי לאדם או לא לקבלו לעבודה על סמך ניתוח ממוחשב של התנהגות העבר שלו.

דברי ההסבר מספקים מספר דוגמאות למידע שאין לבסס עליו החלטות באופן אוטומטי:

המגבלות אינן חלות על עיבוד הנדרש בכדי לעמוד בחוזה בין נשוא המידע לשולט בו או עיבוד שנעשה בהסכמתו המלאה של נשוא המידע.

ככלל, אין לעשות שימוש בקטגוריות מיוחדות של מידע (בין היתר דעות פוליטיות, דת, מצב בריאותי, נטייה מינית) כבסיס לקבלת החלטות.

במידה שנעשה עיבוד אוטומטי לגיטימי יש לנקוט באמצעים מספקים על מנת להגן על שלמות ואמינות המידע כולל היכולת לבצע התערבות אנושית בהחלטה.

23 |המקום והזמן המתאימים

גדפ"ר תפקידו לאחד את ההנחיות בנושא הפרטיות בכל רחבי אירופה. עם זאת, הוא מאפשר לארצות השונות להרחיב ולפרק הנחיות ספציפיות בנושאים כגון ;בטחון לאומי, אבטחה ציבורית, חקירות ואיסוף נתונים הקשורים לחקירות פליליות ויעדים חשובים אחרים בעלי אינטרס ציבורי של כלל האיחוד או המדינה החברה בו.

24 | מי כאן שולט? תפקידו של השולט במידע

אנו מדלגים בצעד קל לפסוק 24, תוך עקיפה זריזה של פסוקים הספציפיים למחוקקים האירופאים אך פחות מעניינים את ישראל ישראלי.

מי שעוקב אחר העלילה מתחילת הדרך, זוכר בוודאי כי בסיפורנו שלושה גיבורים:

1. נושא המידע - האדם הטבעי שהמידע שלו שייך לו;
2. השולט במידע - הארגון שבא במגע ישיר עם המידע, אוסף אותו ומשתמש בו;
3. מעבד המידע - התומך בשולט אך לא אחראי על האיסוף והשימוש במידע באופן ישיר.

הפסוק עוסק בחובות השולט במידע מציג אמירות כלליות הצורכות הכרה והבנה מעמיקה של שאר הסעיפים אך גם הבנה וניסיון בניתוח סיכונים וצמצומם.

הפסוק דורש מן השולט במידע:

1. לנקוט בבקרות טכנולוגיות ותהליכיות בהתאם לאופי המידע ורמת הסיכון כי זכויות האדם הטבעי יפגעו;
2. להיות מסוגלים להוכיח בכל עת כי הבקרות השונות הנדרשות ברגולציה מבוצעות בהתאמה לדרישות;
3. להגדיר מדיניות להגנה על המידע וליישמה בהתאמה לדרישות הרגולציה;
4. לפרסם ולדבוק בקוד התנהגות ארגונית - על כך נרחיב כשננתח את פסוק 40 (יש למה לחכות);

דברי ההסבר מספקים מספר דוגמאות לסיכונים: אפליה, נזק פיננסי, נזק תדמיתי, אובדן החשאיות או כל נזק כלכלי או חברתי משמעותי אחר.

השולט והמעבד במידע

25 | לתכנן את הפרטיות מהתחלה, כי אין ברירה

הפסוק עוסק בגישה מהפכנית שקשה להבנה בתרבות הישראלית - קודם מתכננים ורק אחר כך מבצעים.

תכננו את היבטי הפרטיות עבור כל שירות חדש, פנימי או חיצוני.

גם פה, כמו בפסוק הקודם, דורשים מאתנו לחשוב ולהתחשב ברמת הסיכון ואופי המידע כדי למצוא את הדרכים היעילות בהן נוכל להגן על המידע.

יש לאסוף את המידע הנדרש בלבד, לשמור אותו לפרק זמן קצר ככל האפשר, ליישם מנגנוני אבטחה ראויים.

והעיקר - אם לא נאמר אחרת יהיה המידע זמין לבעל המידע בלבד.

בזכויות נושא המידע (הסכמה, הזכות להישכח וכאלה)...

היבט נוסף, מעניין וחשוב, שאנו לומדים מהפסוק שלנו הינו הדרישה לקבוע פרטיות כברירת מחדל. תתחילו מהנקודה המינימלית: הכל סגור אלא אם כן נדרש באופן ספציפי לפתוח אותו.

קחו למשל רשת חברתית כזו או אחרת. (נקרא לה ספר הפנים או קשר פנימי). ברירת המחדל צריכה להיות כי כל פוסט שנפרסם יהיה חשוף לנו בלבד (אתם רואים את הפוסט הזה? אופס....).

26 | יחד יד ביד נשלוט על המידע

ומה קורה עם יש יותר מגוף אחד אשר שולט על המידע? יחלקו!

הפסוק מדבר על משמורת משותפת של שני גופים השולטים במידע פרטי.

על הגופים להסכים ביניהם על חלוקת האחריות למימוש זכויות נושא המידע ולוודא כי שום דבר לא יפול בין הכיסאות.

יש לתעד בצורה ברורה חלוקה זו כך שבעל המידע ידע למי לפנות באיזה עניין.

27 | מי מציג במאי באירופה? הנציג שלך!

חזרה קצרה לאירועי הפסוקים הקודמים.

ארגונים עליהם חלה הרגולציה: כל ארגון המציע סחורות או שירותים באירופה, בתשלום או ללא תשלום, או כזה העוקב אחר התנהגותם של אנשים אשר שוהים באירופה.

מי שעונה לפחות לאחד משני התנאים האלה, חלה עליו הרגולציה, לרבות הנושא אליו מתייחס הפסוק שלנו היום.

והתנאי שנוסף בפסוק 27: על השולט ומעבד המידע למנות נציג לפחות באחת ממדינות אירופה שבהן מתבצע השירות.

על הנציג לקבל מינוי פורמלי, בכתב, ולהוות כתובת אליה יופנו כל הבקשות והתלונות לגבי עמידה בדרישות הרגולציה.

מינוי הנציג אינו מפחית את האחריות הישירה של השולט או המעבד של המידע אלא מאפשרת לזרועו הארוכה של המחוקק האירופאי להגיע עד לביתכם.

יוצאים מן הכלל שאינם נדרשים להציג נציג הינם ארגונים המספקים שירותים הניתנים באופן חד פעמי ואינם עוסקים בכמות רבה של מידע פרטי וכן אינם כוללים מידע רגיש.

ארגונים בינוניים וקטנים - שימו לב לדרישה זו. נא להתנהג בהתאם!

28 | שרשרת האחריות - אם אין הסכם, חבל לכם

זוכרים את הפרסומת ההיא על החברים שלכם והחברים של החברים? אם לא, אז אתם כנראה צעירים ומאושרים. בכל מקרה, כדי שתצאו צדיקים, כדאי שתהיו מכוסים.

מדובר על יחסי הגומלין בין האחראי לעיבוד - המכונה קונטרולר - לבין מי שנותן לו שירות - המכונה פרוססור.

החוק דורש כי המעבד יתחייב באופן חוזי ומפורט כי הוא עומד בדרישותיו. יש להוסיף נספח לחוזה אשר מתחייב לעמוד בדרישות אלה. (פסוק 28, אם דווקא בא לכם לחזור למקורות).

הספקים שלכם לא ישושו לתת לכם הסכם כזה, אבל, אם תבקשו, הרציניים שבהם יספקו מסמך שהוכן ונחתם מבעוד מועד וכל מה שנותר לכם זה לחתום עליו. (במקרים רבים באופן מקוון).

אם הספק היקר שלכם לא יניח על שולחנכם הסכם כזה, כדאי לכם לחשוב רגע האם בא לכם לחטוף תביעות בגללו.

הפסוק האמור מפרט מה בדיוק צריך להיות בהסכם. ניתן לראות דוגמאות לכך אצל הספקים הגדולים כמו AWS (חפשו ערך DPA או Data Protection Amendment)

29 | אל תגיד נגיד

שיהיה ברור. מעבדים יקרים (יענו פרוססורים). אל תעשו מה שלא אומרים לכם! אחרת אתם מפירים חוזה וגם חוק.

דאגו לקבל הנחיות ממש ממש ברורות ומתועדות מהבקרים (הקונטרולרים) שלכם מה עליכם לעשות עם המידע ותעשו אך ורק את זה.

30 | החיים מתחילים בפסוק 30. אם לא תדעו מה יש לכם, לא תוכלו לצאת למסע

בספר שלנו, כמו בספרים אחרים, אין מאוחר ומוקדם. באופן מפתיע, פסוק 30 אליו הגענו היום הוא נקודת הפתיחה הנכונה למסע במחוזות ה-GDPR.

על כל ארגון השולט במידע או מעבד אותו לתחזק באופן שוטף רשימה פורמלית, מסודרת, מפורטת ומעודכנת של כל תהליכי העיבוד שלו תוך דגש על כאלה המחזיקים מידע פרטי, זכרו שההגדרה למידע פרטי רחבה מאוד.

על רשימה זו להכיל לפחות את השדות הבאים:

1. שם השולט/ מעבד המידע ופרטיו
2. מטרת העיבוד
3. קטגוריות המידע השמורות בתהליך
4. למי יועבר המידע
5. פירוט המדינות מחוץ לאירופה אליהם יועבר המידע
6. אורך חיי המידע
7. תיאור הבקרות הטכנולוגיות והתהליכיות שנועדו להגן על המידע

אז עכשיו, כשאתם יודעים איפה אתם חיים, ניתן לצאת לדרך בבטחה. שיהיה לכם מסע קל ונעים!

31 | פיקוח ללא קיפוח - מי נגד מי?

פסוק 31 הינו קצרצר ופשוט לכאורה: הוא דורש כי השולטים במידע פרטי של תושבי אירופה והמעבדים אותו ישתפו פעולה עם הרשויות להן סמכות הפיקוח על יישום הרגולציה.

נותרה רק שאלה אחת קטנה: ארץ הקודש אינה באירופה (למעט בתחרויות ספורט כאלה ואחרות). אז מי סמכות הפיקוח הרלוונטית עלינו?

לאחרונה שומעים רבות על רשות הגנת הפרטיות אשר פעילה מאוד בתחום אחריותה. אך רשות זו כפופה לחוקי מדינת ישראל ולא לחוקים האירופאים.

אבל הרגולציה מגדירה כי היא תקפה לכל מקום בעולם בו מעבדים מידע פרטי של אזרחי אירופה. אז מי כאן אחראי?

חלק מהפתרון נמצא בפסוק 27 אותו ביקרנו לא מזמן. פסוק זה דורש כי כל ארגון הרלוונטי לרגולציה והוא נמצא מחוץ לאירופה יקים נציגות באירופה.

לנציגות תהיינה סמכויות מוגדרות ומתועדות והיא תהיה הכתובת לתלונות.

ומי מבטיח שבאמת תהיה נציגות כזו? ומי מבטיח שאכן ניתן יהיה ללכוד את מפרי החוק באמצעות השלכת החכה לנציגות המקומית?

ימים (והרבה עורכי דין) יגידו.

במקומות אחרים וגם כאן מהעיר נשמע קול קורא:הבינו נהלי אבטחת מידע, קבלו אסמכה לתקן כלשהו (27001 או מספר חזק אחר) והרי אתם מוכנים ל-GDPR ,תקנות הפרטיות ושאר ירקות מגינת הפרטיות.

כמה בעיות קטנות עם התזה הזו:

- הזנב מקשקש בכלב? אבטחת מידע, חשובה ככל שתהיה, היא רק חלק מעולם הפרטיות. במקרה של GDPR מדובר על פסוק אחד מתוך 99.

  התקנות הישראליות החדשות מתייחסות אך ורק לאבטחת מידע, אבל, שימו לב - זהו עדכון לחוק הפרטיות הוותיק (שהקדים את זמנו). חוק רחב ומקיף שגם בו אבטחת מידע היא רק חלק מהסיפור.

- אין תהודה לתעודה. בהמשך למה שנכתב למעלה, תעודה כזאת או אחרת אינה מקובלת כחותמת בשרות, מה שצריך לעשות זה לעשות.

32 | האבטחה שבפרטיות או הפרטיות שבאבטחה

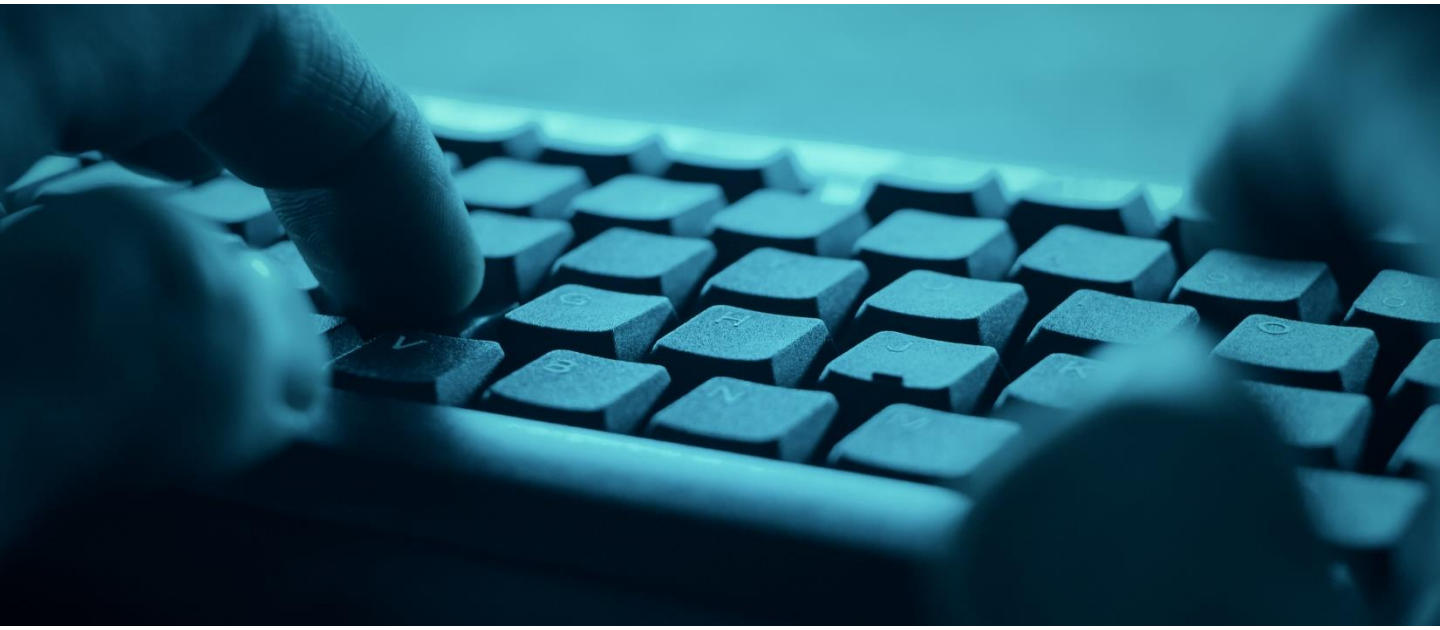
עשית ולא בדקת לא עשית. פסוק 32 של - GDPR הפסוק הממוקד באבטחת מידע - דורש לבצע בדיקות תקופתיות של אבטחת המידע. התקנות הישראליות דורשות בפירוש לבצע מבדקי חדירה (מה שנקרא PT). אל תוותרו על זה!

אז מה כלול במה? אבטחת מידע בפרטיות או פרטיות באבטחת מידע? רמז - התשובה היא כן

33 | יש לך הודעה: המידע התאדה

פסוק 33 דורש מהשולטים במידע להודיע לרשות הפרטיות המתאימה במידה ומידע פרטי דלף להם בין הידיים. יש לשלוח את ההודעה תוך לא למעלה מ-72 שעות. אם לא ניתן לבצע זאת בפרק זמן זה, יש להצטייד בתירוץ טוב.

על ההודעה לכלול את אופי המידע שדלף, המספר המשוער של נושאי המידע שנפגעו, אנשי הקשר הרלוונטיים, ההשלכות האפשריות מדליפת המידע והצעדים המתוכננים על מנת לצמצם את הנזק. גם אם בשלב ראשון לא כל המידע זמין, ניתן לעדכן את ההודעה בשלבים. יש לתעד את פרטי הדליפה, הנזק שנגרם והמהלכים שבוצעו לצמצם את הנזק.



34 | יש לך למי שדאג שהמידע זלג, מודיעים לך ביגון שזה אכן נכון

בפסוק 33 דאגנו ליידע את רשות הפרטיות, תהיה אשר תהיה, כי מידע פרטי דלף לנו.

היום מזכירים לנו את העיקר: למי שייך המידע? יפה אמרתם, לנושא המידע. לכן, מן הסתם, גם הוא צריך לדעת כי המידע שלו היה פרטי ואיננו עוד.

יש להודיע על הזליגה לתושב המאוכזב בלי שיהוי, במידה וזליגת המידע עלולה לגרום נזק משמעותי.

יש לדווח על האירוע בצורה ברורה וקריאה, גם לגברת ון-גברת מהולנד. על ההודעה להכיל מידע דומה לזה שעליו דנו אתמול.

אין צורך לדווח על אירוע זליגה שנחסם על ידי אמצעים יעילים כגון הצפנה.

במידה והמשימה מורכבת מידי וקשה, כאשר הנזק היחסי אינו גדול, ניתן להודיע באמצעי תקשורת ציבוריים.

חושבים שההנחיות מאוד לא חד משמעיות? אתם לא לבד. זה מה יש.

35 | איזה מן סוג של השפעה פועל עלי

אחד מן המנגנונים החשובים אותו מגדיר ספרנו הינו "הערכת ההשפעה של הגנת המידע" – DPIA.

עיבוד מידע אישי בטכנולוגיות חדשות, בהתחשב באופיו, היקפו, ההקשר ומטרות העיבוד, עלול לגרום לסיכון גבוה לזכויותיהם ולחירויותיהם של אנשים. במקרים אלה על הבקר לבצע טרם יישום הפתרון הערכה של ההשפעה של פעולות העיבוד הצפויות על ההגנה על נתונים אישיים.

במיוחד יש לבצע הערכה כזו באשר:

- עיבוד שיטתי ונרחב של מידע המבוסס על ניתוח אוטומטי (פרופיילינג);
- עיבוד בקנה מידה גדול של קטגוריות מיוחדות של נתונים אותן פגשנו בפסוק 9, או של נתונים אישיים הנוגעים להרשעות פליליות ולעבירות (כמה גדול זה גדול? שאלה שאלתית);
- ניטור שיטתי של שטח נגיש לציבור בקנה מידה רחב.

ההערכה תכלול לפחות:

- תיאור שיטתי של פעולות העיבוד הצפויות ומטרות העיבוד;
- הערכת הנחיצות והמידתיות של פעולות העיבוד ביחס למטרות;
- הערכת הסיכונים לזכויות ולחירויות של נושאי נתונים והצעדים המתוכננים לטיפול בסיכונים, לרבות אמצעי הגנה, אמצעי אבטחה ומנגנונים להבטחת ההגנה על נתונים אישיים והוכחת עמידה בתקנה זו תוך התחשבות בזכויותיהם ובאינטרסים הלגיטימיים של נושאי נתונים ואנשים אחרים הנוגעים בדבר.
- במידת הצורך, הבקר יבקש את דעתם של נושאי הנתונים או נציגיהם לגבי העיבוד המיועד, מבלי לפגוע בהגנה על אינטרסים מסחריים או ציבוריים או באבטחת פעולות העיבוד.
- במידת הצורך, יבצע הבקר בדיקה על מנת להעריך אם העיבוד מתבצע בהתאם להערכת השפעת הגנת הנתונים לפחות כאשר יש שינוי בסיכון שפעולות העיבוד מייצגות.

36 | צמצום הסיכון לא מסתדר? יש עם מי לדבר

בפסוק 35 למדנו כי עבור תהליכים בהם מידע פרטי רגיש עלינו להעריך את הסיכונים הכרוכים בעיבוד המידע, לתכנן וליישם את התהליכים והטכנולוגית לצמצומם. נא להתנהג בהתאם! זהו תהליך חשוב ומחייב.

מה קורה אם הסיכון גבוה, ארוכה הדרך ואין כסף למסע ועל כן איננו יכולים ליישם הגנה נאותה?

חובה וגם זכות השולט ליצור קשר במקרה זה עם רשות הפרטיות הרלוונטית (לא שכחנו - בהמשך נדון בשאלה - מי היא רשות עלומה זו?).

רשות זו מחויבת לייעץ לארגון ולהגדיר מה על השולט והמעבד לעשות ולספק המלצות בכתב תוך פרק זמן שלא יעלה על שמונה שבועות.

יש לספק לרשות מידע מפורט לגבי אופי העיבוד, מטרתו, הדרכים בהן המידע מוגן, ההסכמים החוזיים לגבי מידע זה וכן מסמך ניתוח הסיכון.

דברי ההסבר מזכירים לנו שלרשות הפיקוח זכות לאסור בכל עת על המשך העיבוד במידה והסיכון הנותר גבוה מידי.

37 | תפקיד חדש בא למדינה - קצין הגנת המידע

שני הפסוקים הבאים יספרו לנו מה מיצובו ותפקידיו של הקצין שלנו. פסוק זה עונה על השאלה מתי בכלל חובה למנות בעל תפקיד כזה.

ובכן, הן על השולט והן על המעבד למנות קצין הגנת המידע באשר:

1. מדובר בגוף ציבורי
2. פעילות הליבה של הארגון עוסקת בניטור מידע פרטי בכמויות גדולות
3. פעילות הליבה של הארגון עוסקת בקטגוריות מידע רגיש (כמוגדר בפסוקים 9 ו-10)

ניתן למנות בעל תפקיד אחד לקבוצה של מספר חברות.

יש למנות לתפקיד אדם בעל כישורים מתאימים. בפרט הכרה של דרישות החוק ויכולת ביצוע המשימות (עליהן נלמד ביומיים הקרובים).

החוק מציין בפירוש כי חברות ייעוץ כמו זו בה עובד המדריך שלכם יכולות למלא פונקציה זו.

יש להודיע לרשות הפרטיות הרלוונטית מי נושא התפקיד.

38 | קצין וג'נטלמן - מעמדו של קצין הגנת המידע

בפסוק הקודם פגשנו את קצין הגנת המידע והגדרנו מתי נדרש למנות בעל תפקיד כזה. (מכאן ואליך אפנה אל הקצין בלשון זכר אבל קצינות מתקבלות בשמחה ובברכה).

בפסוק זה מוגדר מעמדו של הקצין היקר בארגון, על הארגון לוודא כי הוא מעורב בכל דבר הקשור בהגנה על מידע פרטי.

יש לספק לו את המשאבים הנדרשים למילוי תפקידו וכן לדאוג כי ישמור על רמתו המקצועית.

יש לשמור על עצמאות הקצין כך שלא יקבל הנחיות מאף גורם בארגון , לא ייענש בעקבות מילוי תפקידו וידווח לרמה הגבוהה ביותר אצל המעבד או השולט במידע.

אנשים פרטיים (נושאי המידע) יכולים לפנות בכל עת אל הקצין שלנו בנוגע לזכויותיהם.

יש להחתים את הקצין על הסכם שמירת חשאיות.

הקצין יכול למלא משימות נוספות כל זמן שלא יהיה ניגוד עניינים בין משימות אלה לתפקידו כקצין הגנת המידע.

39 | דרכיו של קצין הגנת המידע

בשני הפסוקים הקודמים למדנו מתי יש למנות קצין הגנת מידע ומה מעמדו בארגון.

עכשיו, כשיש לנו, בשעה טובה, קצין בסביבה, מה המשימות שלו? מה יעשה לו את זה?

אז ככה:

- להנחות את הארגון ועובדיו בכל הכרוך ברגולציה זו והרגולציות המקומיות בנושא פרטיות.
- לנטר את הביצוע של המשימות השונות המבוצעות בכדי לעמוד בדרישות, כולל מעקב אחר רמת הביצוע, המודעות וההבנה של כל אחת מן הדרישות.
- לסייע ולייעץ בתהליך סקירת ההשפעה העסקית.
- לשתף פעולה עם הגופים הרגולטוריים.
- להיות איש הקשר לכל עניין עם רשויות האכיפה כולל התייעצות אתם במקרה הצורך.
- על הקצין להיות נבון, נבון תמיד, לקבל החלטות על בסיס הסיכון הכרוך בכל פעולה הקשורה בטיפול במידע אישי.

40 | לפצח את קוד ההתנהגות

פסוק 40 מציע הצעה שלא כדאי לסרב לה: חברים, כתבו מסמך עקרונות ליישום הגנת הפרטיות בארגון שלכם. מסמך זה יהווה קוד אתי שהארגון מתחייב לעמוד בו (מה שמכונה בלעז קוד אוף קונדקט).

המסמך יצהיר על הדרך בה אתם מתמודדים עם הדרישות השונות של הרגולציה כגון זכויות נושאי המידע, רישום וניהול רשומות, מחזור החיים של המידע, אבטחת המידע ועוד.

הרגולציה מציעה לפתח נוסח מקובל של הצהרות מסוג זה על ידי קבוצות מסקטורים או תחומי עניין שונים אשר יאושרו על ידי גופי הפיקוח.

מסמכים אלה ישמשו בעתיד כבסיס להסכמה פורמאלית על ידי גופים שיוסמכו לכך.

בינתיים זו הצהרת כוונות בלבד, אבל אני מאמין שכדאי מאוד להיערך בהתאם.

בכל מקרה, המסמך יעשה לכם סדר בארגון, יביא למחויבות ההנהלה וכן יהווה אסמכתא רשמית לפעילותכם הברוכה בתחום.

שימו לב שלאורך היצירה פרוסים לא מעט אזכורים של המסמך המדובר.

בפועל, מניסיוני, לא ראיתי יותר מידי שימוש במסמך זה וכן רמת ההיענות לבקשת אישור כזה מהמחוקקים האירופאיים אינה גבוהה.

41 | מי מחליט שהקוד טוב מאוד?

בפסוק הקודם דנו על קוד ההתנהגות. הסעיף שלנו היום שואל - מי מוודא שהקוד מספיק טוב?

הסופר מבהיר לנו כי גוף כזה צריך לעמוד בתנאים הבאים:

- הוכיח את עצמאותו ומומחיותו ביחס לנושא הקוד לשביעות רצונה של הרשות המפקחת המוסמכת;
- קבע נהלים המאפשרים לו להעריך את זכאותם של בקרים ומעבדים הנוגעים בדבר להחיל את הקוד, לפקח על עמידתם בהוראותיו ולבדוק מעת לעת את פעולתו;
- קבע נהלים לטיפול בתלונות על הפרות של הקוד או על אופן ביצוע הקוד
- הוכיח לשביעות רצונה של הרשות המפקחת המוסמכת כי משימותיה ותפקידיה אינם גורמים לניגוד עניינים.
- ינקוט בפעולות מתאימות במקרים של הפרת הקוד על ידי בקר או מעבד, כולל הסרה או אי הכללה של הבקר או המעבד הנוגעים בקוד.

רשות הפיקוח המוסמכת תבטל את הסמכתו של גוף כאמור בסעיף 1 אם הדרישות להסמכה אינן מתקיימות, או אינן מתקיימות עוד, או כאשר פעולות שביצע הגוף מפרות תקנה זו.

אני שוב מדגיש, לעת עתה לא ראיתי שימוש יותר מידי רחב במנגנון זה.

42 | חותמת בשרות על האש

אני שוב ושוב נשאל: מי יכול להסמיך ארגון לכך שהוא עומד בדרישות הרגולציה?

התשובה המידית, נכון לעכשיו, היא שיש רק ארגון אחד בעולם שיסמיך אתכם. והארגון הזה הוא אתם.

אין היום תעודות, חותמות והסמכות מוכרות על ידי הרגולציה, לא עבור אנשים ולא עבור ארגונים.

אם מצאתם כזה, מה טוב ומה נעים לכם. כדאי, בכל מקרה, לקרוא את תנאי השימוש ולוודא מי הסמיך את המסמיכים . אבל, יש לכם מזל: צאו בריקודים כי הבשורה מהממת - הולכת ומתקדמת החותמת!

הרגולציה מעודדת הגדרה של חותמת כשרות כזו במיוחד עבור ארגונים קטנים ופצפונים. היא קוראת למדינות השונות לאשר מסגרת כזו .הדבר לא יחליף חוזים משפטיים כופים כגון הסכם העברת מידע לארצות זרות.

יתרה מזו, תעודות, חותמות וקמיעות אחרות לא יסירו מכם כהוא זה את האחריות אם חלילה ימצא פער בין ציפיות החוק למה שאתם עושים הלכה למעשה.

ניתן יהיה להנפיק תעודות כאלה לפרק זמן של עד שלוש שנים, לאחר מכן יפוג תוקפן.

כאן המקום להזכיר לכם את הפסוקים 40 ו- 41, אותם קראנו רק לפני מספר ימים.

חברים, עשו לעצמכם טובה ותפתחו קוד אוף קונדקט (למי שהפסיד את השיעור - שידור חוזר בפוסטים הקודמים שלי).

43 | עוד על הסמכות - מי סומך על המסמיך?

דיברנו רבות על הסמכות ומסמיכים ועלה כאן טיעון כי זה הולך להיות שוק פרוע ולא מבוקר.

אז זהו שממש ממש, אבל ממש לא!

פסוק 43 מגדיר ברחל ביתך הקטנה מי ראוי להסמיך ארגונים (כאמור, בשלב זה זוהי הצהרת כוונות אבל אם תמתינו בסבלנות זה בוא יבוא):

- יאושררו באופן פורמאלי על ידי הרשויות האירופאיות או אלה במדינות השונות (בדומה לאקרדיטציה של תקני איזו).
- יוכיחו את העצמאות וחוסר התלות שלהם בגורמים המוסמכים.
- יגדירו תהליכים להענקת תעודות, חותמות ואישורים וכן מדדים לשלילתם. תהליכים אלה יוצגו לרשויות ויאושרו על ידיהן.
- ימסדו תהליך לקבלה וטיפול בתלונות על אי עמידה בתקנים.

תהליך ההסמכה יבוצע למקסימום חמש שנים (לחדי העין - בסעיף קודם דובר על שלוש שנים. מה תופס?).

במידה וגופי האסמכה לא יעמדו בדרישות הנ"ל ניתן לשלול את האשרור שלהם.

44 | יציאת אירופה - כשהמידע יוצא אל הלא נודע

הפסוק שלנו, שמספרו 44, פותח מחרוזת העוסקת בהעברת מידע מחוץ לגבולות אירופה.

זה אך טבעי שהמידע של פרטים באירופה יזרום לארצות אחרות כחלק מסחר בינלאומי ושיתוף פעולה חוצה גבולות.

יחד עם זאת, האירופאים לא מוכנים לזרום עם זה כל עוד ולא יובטח כי עם הגיע המידע לביתו החדש, הוא יזכה לטיפול חם ואוהב, ובעיקר בטוח, כמו בארץ מולדתו.

הפסוקים הבאים מרחיבים את הדרישות והתנאים על מנת שהם יסכימו למסור למידע את ברכת הדרך.

45 | להיות או לא להיות מדינות ראויות

חזרנו למסלול ואנו ממשיכים לעסוק בנושא העברת מידע מחוץ לאירופה.

פסוק 45 מסביר את אחד המנגנונים המאפשרים להעביר מידע. זהו מבחן ההלימה (אדקוווסי בלעז).

זוהי "חותמת כשרות" למדינות המגנות על המידע כראוי. בהינתן חותמת זו אין צורך באישור נוסף.

חותמת כזו ניתנת למדינות אשר:

- קיימת בהן מסגרת משפטית הולמת לגבי הגנה ראויה על המידע, העברתו לארצות זרות והגנה על זכויות נושא המידע.
- קיום גוף אכיפה חזק המוודא עמידה במסגרת חוקית זו.

הרגולטור האירופאי בוחן את עמידת המדינות המאושרות בדרישות לפחות פעם בארבע שנים.

הרגולטור יכול בכל רגע נתון להחליט לבטל את האישור במידה ויתגלו חריגות משמעותיות. ומי במאושרים? לא תאמינו. אנחנו שם! יחד עם אנדורה, איי פרעה, גורנסי, ג'רסי, ניו זילנד, אה... וגם קנדה, שוויץ וכאלה. סך הכל 10 ארצות בלבד (חלקן הגדול ארצות ארצות).

46 | רבות הדרכים לשלוח מידע למרחקים

ב-9 ביולי 2019 נפתח דיון בבית הדין לצדק של האיחוד האירופי בלוקסמבורג בתיק המכונה Schrems II. זהו פרק ב' של תלונה שמקס שרמס, סטודנט אוסטרי צעיר שעומד בראש תנועה שחרתה על דיגלה את הסיסמא "זה לא העסק שלך" העלה חמש שנים קודם לכן.

מקס תבע את פייסבוק על כך שהיא אפשרה לרשויות בארה"ב גישה לנתונים האישיים שלו בניגוד לחוק הגנת המידע של האיחוד האירופי. מקרה זה הפך לפסק דין מקדמי והביא לביטול מסגרת ה "סייף הארבור" - מנגנון שחברות רבות הסתמכו עליו בכדי לתת לגיטימציה לזרימת מידע פרטי מהאיחוד האירופי לארה"ב.

שנה לאחר מכן שרמס החליט לערער גם על ההעברות שבוצעו על בסיס מנגנון אחר - "סעיפים חוזיים תקניים" - המנגנון האלטרנטיבי שפייסבוק בחרה להסתמך עליו כדי לתת לגיטימציה לזרימת מידע ממדינות האיחוד האירופי לכיוונה.

פסק הדין הגיע - והוא היכה למוות את הסדר זרימת הנתונים מהאיחוד האירופי לארה"ב שנקרא "מגן פרטיות". פסק הדין קבע כי "ההסדר הקיים פוגע בזכויות היסוד של אנשים שהנתונים שלהם מועברים למדינה שלישית", קבע המחוקק. "המנגנונים הקיימים שנועדו לכאורה להפחית את הסיכון אינם עומדים בדרישות החוק האירופי".

פסק הדין בפרשה זו עלול לגרום לרעידת אדמה משמעותית בנוף הגנת המידע של האיחוד האירופי, מכיוון שהוא עלול לגרום לביטול המנגנון הנפוץ ביותר לצידוק העברה של מידע אישי מהאיחוד האירופי למדינות אחרות. ההחלטה עשויה להשפיע גם על תקפותם של מנגנוני העברה אחרים, כמו ה "פרייבסי שילד" של האיחוד האירופי -ארה"ב, שהחליף את ה "סייף הרבור", ובכך יישארו לחברות חלופות מוגבלות בכדי להצדיק זרימת מידע מחוץ לגבולות האיחוד האירופי.

פרשת שרמס II נוגעת באופן ישיר לפייסבוק, אך יש לה השלכות רחבות מאוד על האופן בו ניתן יהיה לבצע עיבוד נתונים של אזרחי האיחוד.

הדגש הוא על העברת נתונים מהאיחוד האירופי לארה"ב. לכן השפעה ישירה של פסק הדין תהיה שיותר חברות אמריקאיות יעברו לעיבוד נתונים אזורי עבור משתמשים באירופה.

הסכם "מגן הפרטיות" החליף את הסכם העברת נתונים קודם שנקרא Safe Harbor, שנקבע ב-2015 לאחר אתגר קודם שהציב אותו שרמס עצמו מול בית המשפט האירופי. לגבי מנגנון אחר - חוזים סטנדרטיים - קבע בית המשפט כי זהו מנגנון מקובל.

יחד עם זאת הוא אינו מספיק כדי לאשר העברת נתונים למדינות שלישיות בהן הגנת המידע אינה מספקת, כמו ארה"ב.

47 | על החוקים ועל הנפלאות אשר חוללו הארגונים

פסוק 47 מציין מה נדרש להגדיר בחוקים תאגידיים מחייבים (ביינדינג קורפורייט רולז).

תזכורת - זוהי אחת מן הדרכים שבאמצעותן ניתן לאשר העברה של מידע אישי אל ארגונים ומארגונים הנמצאים במדינות שלא אושרו בתהליך ההלימות (אדקווסי).

חוקים כאלה צריכים, בין היתר:

1. להיות תקפים על כל הארגונים הרלוונטיים כולל עובדיהם
2. להבטיח כי מוענקות זכויות לנושאי המידע
3. לפרט את המידע המועבר, מטרת המידע, יעד ההעברה
4. להגדיר את יישום עקרונות החוק: הגבלת מטרת ההעברה, שמירת מינימום מידע הכרחי, שמירה לפרק זמן קצר ככל האפשר, מידע אמין ומוגן כראוי
5. להצהיר בצורה מפורשת על קבלת אחריות על כל פריצה למידע אלא אם כן הוכח כי הארגון אינו אחראי לכך
6. למסד מנגנוני ביקורת ובקרה עצמית
7. להבטיח קיום הדרכה והכשרה מתאימים
8. להגדיר את התפקידים והאחריות של קציני הגנת המידע

48 | להעז לסרב גם כשעיני כל האומה נשואות אליך

פסוק 48 מעלה נקודה חשובה, מעניינת ואפילו, הייתי מעז לומר, אמיצה.

גם אם מדינה זרה פונה לשולט או המעבד של המידע בתביעה להעביר אליה מידע אישי השמור אצלה תיכף ומיד וללא שיהוי, הגוף אינו בהכרח מחויב לעשות זאת.

העברת המידע תתבצע אך ורק אם קיים הסכם בינלאומי תקף בין המדינות המאפשר העברה של מידע מסוג זה.

זוכרים אחד, סנודן, שחשף את כלי המעקב הנפלאים של סוכנות האבטחה האמריקאית כגון תכנית פריזם? תכניות אלה אפשרו מעקב אחר מיליוני משתמשים בדואר אלקטרוני, שירותי טלפון, משחקים וכאלה.

אז זהו שעבשיו אולי זה יהיה טיפה יותר מורכב או לפחות לא ממש מקובל לבצע דברים כאלה, לפחות לגבי תושבי אירופה.

49 | דרכים צדדיות - ואף על פי כן מעבירים מידע

בפסוקים הקודמים למדנו על תנאים שונים שבמידה והם מתקיימים ניתן להעביר מידע מחוץ לגבולות אירופה.

מה קורה אם אף אחד מאלה לא מתקיימים אך בכל זאת אנו מעוניינים כי המידע ינוע? כלום לא קורה, הכל כרגיל .... אלא אם כן:

- יש הסכמה מפורשת של בעל המידע להעברתו
- ההעברה נדרשת לקיום חוזה בין בעל המידע למעבד שלו
- המידע חיוני מסיבות חשובות לעניין הציבורי (מה חשוב היום?)
- המידע נדרש על מנת להגן על אינטרסים חשובים של נושא המידע (למה חשוב? למי חשוב?)
- ניתן להעביר בתנאים אלה מידע מוגבל בלבד וכל זאת לאחר בדיקה המוודאת כי המידע ישמר באופן קפדני ללא פגיעה בזכויות בעל המידע.

50 | כולנו ביחד, תנו צ'אנס לפרטיות

הגענו לפסוק חמישים. חצי מאה עברה. זהו פסוק אופטימי על שיתוף ואחווה.

הבה נשב יחד, אומר לנו הפסוק, הארצות, הארגונים ומערכות הפיקוח מכל העולם ונעודד:

1. מכניזם לשיתוף חוקים ואכיפה בנושא הפרטיות
2. עזרה הדדית, שיתוף מידע, התראות והודעות חוצות גבולות
3. עירובם של מובילי דעה מכל קצווי תבל בהובלת המהפך

יחידות פיקוח עצמאיות

51 | האיחוד האירופי - קיצור תולדות הזמן

25 הפסוקים הבאים דנים במנגנונים של האיחוד האירופי. זה פחות רלוונטי אלינו אבל אנו נמשיך בטיולנו, ולו רק כמחקר אנתרופולוגי מעניין.

שורשי האיחוד האירופי לאחר מלחמת העולם השנייה. היעד היה ועודנו לאפשר תנועה בלתי מוגבלת של אנשים, סחורות, כספים ושירותים בין המדינות החברות.

לאיחוד מאפיינים רבים של מדינת על, בדומה לארצות הברית, ובנושאים אחדים הפיקוח המרכזי אף הדוק יותר, כולל בנושא שלנו - הגנת הפרטיות.

באיחוד 27.5 מדינות (אנגליה בדרך החוצה - הברקסיט המדובר) ומספר מדינות המחכות כבר שנים לצירוף.

ארבעת המוסדות העיקריים באיחוד: המועצה האירופית, מועצת האיחוד, הפרלמנט והנציבות.

הנציבות הינה הרשות המבצעת והיא אחראית בעיקר לתיאום ופיקוח.

בסיפור שלנו נוספים מוסדות ייחודיים בנושא הפרטיות. בכל מדינה הוקמה רשות הגנת פרטיות מרכזית.

רשויות אלה מתואמות ביניהן וכן עם הנציבות. בנוסף על הרגולציה המקובלת על כולן, רשויות אלה מוציאות הרחבות והבהרות משלהן.

ראויה לציון בעיקר הרשות האנגלית המכונה ico המפרסמת חומר רב וטוב. שימו לב שהאנגלים ימשיכו להיות חזק בעניין גם אחרי הברקסיט.

52-59 | יכולות, משימות ושאר נפלאות

היום זה היום שלכם! אתם מקבלים חמישה פסוקים במחיר של פוסט אחד.

הפסוקים עוסקים ביכולות של גופי הפיקוח במדינות השונות באיחוד ויחסי הגומלין ביניהם.

גופי הפיקוח בכל מדינה אחראים על השולטים במידע והמעבדים אותו בגבולותיהם.

הם אמונים על טיפול בתלונות, ביצוע חקירות והעלאת המודעות, הדרכה והכוונה של ארגונים ופרטים.

כמו כן הם אחראים על בחינה ואישור של קודי התנהגות (קוד אוף קונדקט) אותו קוראי הנאמנים מכירים זה מכבר.

במידה ומדובר באירוע המתרחש במספר מדינות, אחת מן המדינות תוביל את הטיפול בו בהתאם לחלקה והחשיבות של האירוע. (על פי עיקרון הוואן סטופ שופ).

לרשויות הפיקוח הזכות לדרוש גישה למידע ולאתרים בו הוא נמצא.

הן יכולות להזהיר את השולט או המעבד של המידע ואף להורות על הפסקת פעולתם.

על כל מדינה להקנות לרשויות הפיקוח זכויות על פי חוק שיכללו לפחות את אלה שברגולציה אך ניתן להוסיף עליהן.

על כל רשות להפיק דוח שנתי שיועבר לפרלמנט המקומי, לממשלה וכן יהיה זמין לעיון הציבור.

שיתוף פעולה ועקביות

60-76 | שיתוף פעולה בשבעה עשר צעדים

קחו אוויר. אנו יוצאים לריצה מהירה. בדרכנו נפגוש 17 פסוקים. אז קדימה, לצמצם רווחים!

הפסוקים שלנו עוסקים בשיתוף פעולה ותיאום בין גופי הפיקוח השונים האמונים על הגנת הפרטיות באיחוד האירופי.

בכל מדינה יכולים להיות אחד או יותר גופי פיקוח ואכיפה. אחד מהם ישמש כמוביל המתאם בין כל האחרים, דואג לשיתוף מידע ביניהם ואומר את המילה האחרונה.

הגופים המובילים של המדינות השונות ישתפו פעולה ביניהם ואף יצאו יחדיו למבצעים נועזים במידת הצורך.

ובראש הגדוד צועד חבר מנהלי הגנת הפרטיות המשותף לכלל המדינות והוא הפוסק העליון בנושאים בעלי משמעות גלובלית כגון מסגרות הסמכה לעמידה בחוק.

חבר המנהלים הינו עצמאי ולא מקבל הנחיות מאף אחד. הוא מבצע פיקוח על, המבטיח את תפקודם התקין של הגופים השונים וכן מספק להם ייעוץ והכוונה.

כמו כן הוא מסייע ומדריך את מוסדות האיחוד האירופי בכל הכרוך בהגנת הפרטיות.

חבר המנהלים הינו גוף דמוקרטי. בראשו עומד יושב ראש נבחר והוא מקבל החלטות על בסיס הצבעות של כלל חבריו.

77 | להתבונן, להתגונן, להתלונן, זה כל הסיפור

המידע שלי, חיובי או שלילי, לא שייך לאיש, אלא אך ורק לי. זה כלל חשוב, בכל העולם, ובאירופה גם.

והאירופאים הגדילו עשות, הקימו פיקוח, השיתו קנסות. עשו רבות להבטיח עכשיו, שחברי הפיקוח נקיים מרבב.

ופקחו אוזניהם לכל תושב האיחוד, שזכויותיו נפגעו או הלכו לאיבוד. ויצאו בקריאה בקול גדול, אם נפגעת חבר, להתלונן אתה יכול.

זמנים עוד יגידו אם היה זה חלום, או מנגנון איכותי שפניו לשלום, שיגן על כל אדם מעצם היותו, על כבודו, הפרטיות שלו ועל חירותו.

זהו סוף הפסוק, אך לא סוף הסיפור.

78 | מי שומר על השומרים?

תיארנו בפירוט את התהליכים השונים שנוקט סיפורנו על מנת להבטיח כי גופי הבקרה והפיקוח על הגנת הפרטיות באיחוד האירופי עושים את עבודתם נאמנה.

ואחרי ככלות הכל, מה קורה אם מר תושב או גברת תושבת אינם מרוצים מהטיפול או מההחלטות של גופים אלה?

אל דאגה. גם לכך דאג המחוקק.

אם הרשויות אינן מטפלות בתלונה או נאלמות דום ליותר משלושה חדשים או, לחילופין, אם החלטותיהן אינן מקובלות על הגברת או האדון, ניתן לפנות לארכאות הגבוהות של האיחוד.

79 | שֹׁפְטִים וְשֹׁטְרִים תִּתֶּן לְךָ בְּכָל שְׁעָרֶיךָ

הפסוק שלנו מציב למר תושב וגברת תושבת כתובת לפניה יוכלו לשטוח את תלונותיהם לגבי הפרת פרטיותם על ידי שולטים ומעבדים.

התלונה תובא לפני בית משפט במדינה בה לשולט במידע או המעבד שלו נציגות.

לחילופין ניתן להביא את התלונה בפני בית משפט של המדינה בו מתגורר המתלונן.

יש שופטים באירופה!

80 | נעים מאוד. מי מציג אותנו?

לנשוא המידע הזכות להסמיך גוף, ארגון או עמותה ללא כוונת רווח הפעילה בתחום ההגנה על זכויותיהם וחירויותיהם של נשואי מידע בכל הנוגע להגנה על הנתונים האישיים שלהם, להגיש את התלונה מטעמו, למימוש הזכויות האמורות בסעיפים 77, 78 ו -79 מטעמו, וכן לממש את הזכות לקבל פיצויים כאמור בסעיף 82 מטעמו אם נקבע בחוק מדינות החברות.

המדינות החברות רשאיות לקבוע שלכל גוף, ארגון או עמותה כזו, ללא תלות במנדט של נושא נתונים, הזכות להגיש, באותה מדינה חברה, תלונה לרשות הפיקוח ולממש את הזכויות אם היא רואה כי זכויותיו של נושא נתונים על פי תקנה זו הופרו כתוצאה מהעיבוד.

ראינו בדיון קודם את פועלו של מקס שרמס שהקים את העמותה "זה לא העניין שלך". שווה לכם לגגל וללמוד על מקס הזועם בדרכים.

81 | שניים אוחזים בתלונה או מחול ל-27.5 רגליים

האיחוד האירופי הוא חיה מורכבת. מצד אחד קיימים חוקים ותקנות חובקי איחוד. מאידך בכל מדינה מוסדות וחוקים שלה.

כיצד מצליח מרבה רגליים בעל 27.5 רגליים לנוע? תשובה נכונה. בזהירות.

במידה וקיימת תלונה דומה על אותו גוף בבתי משפט במדינות שונות, מי שעלה ראשון יתפוס את הפיקוד והאחרים יפנו לו את הדרך.

זה מזכיר לי את הצמתים בחוץ לארץ בהם ארבעה תמרורי עצור. הראשון שמגיע הוא הראשון שעובר.

האם גישה כזו הייתה עובדת בארצנו הקטנטונת בעלת שתי רגליים בקושי? נושא למחשבה.

82-84 | הגיע יום נקם ושילם - כמה זה עולה לנו?

חברים. הגענו לפסוקים שבעקבותיהם העולם בפאניקה - הקנסות והעונשים שיושתו על המפירים את החוק.

כל המדינות באיחוד נקראות לבנות מנגנונים יעילים לקנוס את מפירי החוק בהתאם לחומרת ההפרה.

רמת הקנס תקבע על סמך רגישות הנתונים שנפגעו, כמות האנשים שהושפעו והפעולות שננקטו על מנת לתקן את ההפרה.

אי עמידה בדרישות הקשורות לנושאים הבאים תגרור קנס של 2% מהמחזור של החברה או 10 מיליון יורו - הגבוה בין השניים:

הסכמה הורית לשימוש במידע ילדים, הגנת המידע משלב התכנון, מילוי תפקידו של קצין הגנת המידע ועוד.

אי עמידה בדרישות הקשורות לנושאים אלה תגרור קנס של 4% מהמחזור או 20 מיליון יורו, הגבוה מבין השניים:

פגיעה בעקרונות היסוד, שמירה על מידע מקטגוריות רגישות, זכויות נושאי המידע, העברת מידע מעבר לגבול ועוד.

שימו לב. דליפת מידע אינה הסיבה היחידה לקנסות. אבטחת מידע הינה חלק חשוב, אך בהחלט לא היחיד בסיפור שלנו.

85 | כתבו עליך בעיתון הרבה דברים?

פסוק 85 מעלה סוגיה מעניינת: איפה עובר הגבול בין חופש הביטוי לפרטיות?

עיתונאים מתפרנסים ממעקב ופרסום אודות מעשיהם של אנשים מפורסמים יותר ומפורסמים פחות.

אתה קם בבוקר ורואה שאתה מובר ומתחיל ללכת. אתה מחייך לעצמך מעל דפי העיתון בטעם של פעם, מצויץ באתרים החברתיים ומכבב באתרי הרכילות ברחבי הרשת.

זו פגיעה בפרטיות או העולם פשוט שמח לראות אותך?

סיפורנו אינו מספק תשובה ברורה לקוראיו הנאמנים. הוא מגלגל את האחריות לארצות האיחוד ומבקש מהן לחוקק חוקים אשר יספקו מענה הולם לאיזון בין חופש הדיבור לזכות שיעזבו אותנו בשקט.

ומה אתם חושבים? מי בא קודם? הפרטיות או זכות הציבור לדעת?

86 | רשמים מרישומים רשמיים - האם הפרטיות היא לנצח?

הפסוק שלנו עוסק במידע אישי האצור במסמכים רשמיים. מידע זה עשוי להיות רגיש.

האם גישה למידע זה פוגעת בפרטיות? ואם כך, כיצד יש לדאוג לאיזון העדין?

הכותב אינו מספק מענה אלא הוא שוב מעביר את הכדור למדינות האיחוד. שיחליטו הן.

שימו לב שזו אינה הפעם הראשונה שהחלטות קשות אינן חד משמעיות בסיפורנו והפסיקה ניתנת לאחרים.

מכאן שכאשר תסיימו בשעה טובה לקרוא את החוק הכללי אתם מוזמנים לקרוא את החוקים המקומיים בזמנכם החופשי.

87 | עתידה של התעודה. המזהה הלאומי ובעיית הפרטיות

גם בפסוק זה עולה לאוויר שאלה חשובה - מה הטיפול הנדרש במספרי זיהוי או אמצעי זיהוי אחרים הנוקטים על ידי המדינות השונות.

שאלה מצוינת. אז מה התשובה?

אז זהו שגם פה אנו נתקלים באחד מאותם מקומות שבהם האיחוד החליט לא להחליט והשאיר את שיקול הדעת לכל מדינה בפני עצמה.

88 | שלוש ארבע לעבודה - עד לא ידע

עצור! הידעת? המעסיק שלך שומר לא מעט מידע אישי אודותיך.

קורות חייך, ביצועיך, רמתך המקצועית, התחביבים שלך, מצבך הבריאותי, הרגלי הגלישה שלך, החיים שלך באופן כללי וכמובן תנאי העסקתך.

האם הוא באמת נדרש לכל אלה? האם הוא ביקש את רשותך לשמור ולעבד את כל החומר הטוב הזה? על כך נסוב הדיון בפסוקים הבאים.

כהרגלו בימים אלה, הסופר שלנו אינו גוזר גזרות חד משמעיות אלא קורא למדינות האיחוד לחוקק חוקים פרטניים בנושא איסוף ועיבוד מידע הקשור לעבודה.

הוא מדגיש כי יש לתת את הדעת על שמירת כבוד העובד ופרטיותו, איסוף המידע הנדרש בלבד ושקיפות מול העובדים לגבי מה נאסף ומדוע.

89 | ההיסטוריה נשמרת - שום דבר לא אבד, לא נשכח

יחס מיוחד נותן המחוקק למידע אישי אשר נאסף לצרכי מחקר, סטטיסטיקה או שימור היסטורי.

בכלל יש לעשות הכל על מנת ליישם את כל דרישות החוק במקרים אלה ובפרט הקפדה על שמירת מידע מועט ככל האפשר.

כמו כן, במידת האפשר, יש ליישם בקרות נוספות כגון אנונימיזציה של המידע, הצפנתו ובקרות אבטחה ראויות.

יחד עם זאת, במידה וביצוע בקרות אלה יגרום לפגיעה משמעותית במטרות האיסוף והעיבוד, מדינות האיחוד יכולות לחוקק חוקים המאפשרים הקלות.

יש לשים לב כי ההקלות יהיו רלוונטיות לעיבוד האמור. כל שימוש אחר כפוף לחוקים המחמירים.

90 | יצא סוד

המדינות החברות רשאיות לאמץ כללים ספציפיים בהקשר לחובה לשמור על סודיות המידע כאשר הדבר נחוץ ומידתי כדי ליישב בין זכות ההגנה על נתונים אישיים לבין חובת הסודיות.

כללים אלה יחולו רק לגבי נתונים אישיים שקיבל הבקר או המעבד בהקשר בפעילות המכוסה באותה חובת סודיות.

91 | קדוש קדוש

חוקים מקומיים בנושא מידע הקשור לקבילות ומוסדות דתיים בגון כנסיות, עשויים להמשיך ולחול,

ובלבד שהם עומדים בקנה אחד עם תקנה זו.

האצלת סמכויות

92-93 | תקנות, ועדות ושאר ירקות

כמעט רואים את האור - זהו אור הרכבת הדוהרת לעברנו וקוראת בקול גדול: ג'ייי דייי פייי אאררר...

לפני הגרנד פינלה אנו עוסקים בסמכות המוענקת לנציבות האירופאית לתקן תקנות המרחיבות את החוק בכלל ובפרט בנושא הסמכות וחותמות רשמיות המעידות על עמידה בדרישות החוק.

תקנות כאלה יכנסו לתוקפן רק אם במשך שלושה חודשים עוף לא יצייץ והפרלמנט והמועצה האירופית לא יביעו כל התנגדות.

נושא אחר שמוצא את מקומו כאן: לצד הנציבות תוקם ועדה אשר תתמקד בנושא הפרטיות.

94-99 | חזק חזק ונתחזק - סוף שהוא רק ההתחלה

חברים נברך. הגענו יחדיו לסוף המסע המפרך. הייתם איתי יום יום בשלושה החודשים האחרונים. היה ממש כיף אתכם.

העשרים וחמישי במאי 2018 כבר כאן. עברנו משלב הדיבורים לשלב המעשים.

הפסוקים האחרונים בסיפורנו אומרים כי התקנות משנת 1995 בטלות ומבוטלות והחוק שלנו מחליף אותן . תהיה תקופת חסד כלשהי אבל לאחר מכן זהו החוק התופס.

עכשיו רק נותר פרט קטן - להפנים את כל מה שלמדנו יחדיו וליישם אותו...

מקווה שסייענו, ולו רק במעט, להבין את כוונת המשורר ולנוע לעבר המנוחה והנחלה המובטחת למי שמגן על המידע הפרטי שלנו ושל כל בית אירופה.

אודות מרכז הגנת הסייבר של BDO

מרכז הגנת הסייבר של BDO (SECOZ לשעבר), מוביל בתחום הגנת הסייבר ואבטחת המידע בארץ ובחו"ל מאז שנת 2002. המרכז צבר בשנות פעילותו הרבות, ניסיון עשיר אל מול השוק הבינלאומי והמקומי, במגוון רחב של מגזרים, ביניהם פיננסים, תעשייה, ממשלה, הייטק, תשתיות, סטרטאפים ובריאות.

השילוב בין מומחיות בתחומי הסייבר ואבטחת המידע לבין מומחיות בתחומי האסטרטגיה וניהול הסיכונים, מאפשרים לצוות מרכז הסייבר לספק לכל לקוח מענה הוליסטי בגישה ייחודית. צוות המומחים שלנו מבין לעומק את התהליכים והדרישות העסקיות של כל לקוח ויודע לשזור אותם בד בבד עם הדרישות והצרכים הטכנולוגיים. באופן זה, בידינו להתאים את הפתרונות האידאליים עבור כל לקוח, סביבה, מטרה וצורך תוך שמירה על האינטרסים והפעילות העסקית.

בין שירותי מרכז הגנת הסייבר: ניהול הגנת הסייבר ואבטחת המידע, שירותי תקיפה, ניהול סיכוני סייבר של שרשרת האספקה, רגולציה והגנה על הפרטיות, ניהול משברים והמשכיות עסקית, ניהול וניטור אירועי סייבר ואבטחת מידע (MDR) 24/7.

אופיר זילביגר
שותף
מוביל פעילות
הסייבר
הבינלאומית,
BDO
ophirz@bdo.co.il

נועם הנדרוקר
שותף
מנהל פעילות ייעוץ
סייבר גלובאלי
BDO ישראל
noamh@bdo.co.il

גלעד ירון
דירקטור
ראש חטיבת הגנת
המידע והפרטיות
BDO ישראל
gilady@bdo.co.il

למידע נוסף על מרכז הגנת הסייבר: לחץ כאן

אודות BDO ישראל

BDO ישראל הינה פירמת ראיית חשבון ויעוץ עסקי דינמית ובעלת אוריינטציה עסקית, הנמנית על חמש הפירמות הגדולות בישראל. הפירמה נוסדה בשנת 1983 כחלק מהרשת הבינלאומית BDO ומפעילה עשרה סניפים ברחבי בארץ, ובמו כן, דסקים ישראלים בסין, הודו, וייטנאם, ארה"ב ויוראסיה.

הפירמה מעסיקה כיום בישראל מעל 1,600 עובדים ומספקת שירותים למגזר הפרטי, הציבורי והממשלתי ומטפלת בלמעלה מ-300 חברות ציבוריות וקרנות שונות, הנסחרות בבורסות בארץ ובעולם.

שירותי הפירמה כוללים: חשבונאות וביקורת, מיסוי מקומי ובינלאומי, יעוץ פיננסי וכלכלי, ניהול סיכונים, יעוץ וביקורת מערכות מידע, יעוץ סייבר, ייעוץ אסטרטגי, ייעוץ תפעולי לוגיסטי ועוד.