Data Protection - Back to Basics

עו"ד אייל שגיא | עו"ד שיר שושני כץ

על מה נדבר היום?

- נחזור להגדרות בסיסיות
- נבחן את הפרשנות העדכנית שלהם לאור תיקון 13 ועמדות הרשות
- נבחן את הפערים שתיקון 13 יצר מול תקנות אחרות
- נבחן כמה גישות לבעיות הקשות של יידוע ומחיקת מידע עודף

AYR
עמר רייטר ז'אן שוכטוביץ ושות'

ACC Association of Corporate Counsel ISRAEL

BACK TO BASICS

שני, 5.5.2025 | 11:00-12:30 | Teams' webinar

Privacy Agreements

עקרונות בסיס בדיני הגנת הפרטיות – מהלכה למעשה

שיר שושני-כץ, שותפה
מחלקת Law & Tech

אייל שגיא, שותף
ראש מחלקת Law & Tech

ליטל נוף-סבג, יועמ"ש
Director of Legal, Head of IP & Product, Monday.com

אסף גלעד, יועמ"ש
Director of Legal & Compliance, Lusha

לורי דישטניק, יועמ"ש
לאומי פרטנרס; מובילת סדרת Back to Basics -ה
מנהלת פורום שוק ההון, ACC

מנהלי פורום פרטיות וסייבר, ACC

AYR
עמר רייטר ז'אן שוכטוביץ ושות'

CONTROLLER / בעל שליטה

GDPR

- Controller
  - means the natural or legal person… which, alone or jointly with others, determines the purposes and means of the processing of personal data

חוק הגנת הפרטיות

- בעל שליטה במאגר מידע
  - מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוסמך בחיקוק לעבד מידע במאגר מידע או שבעל תפקיד בו הוסמך לכך כאמור

AYR

מיהו בעל שליטה

- GDPR:
  - בעל שליטה לא חייב שתהיה לו גישה פיזית או משפטית למידע
  - גוף יכול להיות בעל שליטה במשותף עקב הסיטואציה
  - לא משנה באיזו מערכת ("מאגר") המידע
  - גוף אחראי כל המידע בארגון
- ישראל:
  - מעבר מרישום להגדרה עצמית, מעבר מ"בעלות" לשליטה
  - שליטה ושליטה משותפת במאגר הן סטטוס לפי המציאות
  - למרות שהרישום לא קונסטיטוטיבי הפוקוס על ההגדרה עובר לחברה / DPO
  - ארגון אחראי על כל המידע שאצלו
  - כל מידע בארגון צריך להיות משוייך ל"מאגר" (כולל מערכת דוא"ל, למשל)

מידע

- "מידע אישי" - נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי
  - "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון
    - שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי
- השלכות של ההגדרה רחבה
  - יותר "מאגרים"
    - כולל יידוע, עיון, אבטחה...
  - יותר גורמים רלוונטים לתקנה 15

AYR

PROCESSOR / מחזיק

GDPR

- Processor
  - means a natural or legal person… which processes personal data on behalf of the controller
- Third party
  - means a natural or legal person… other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

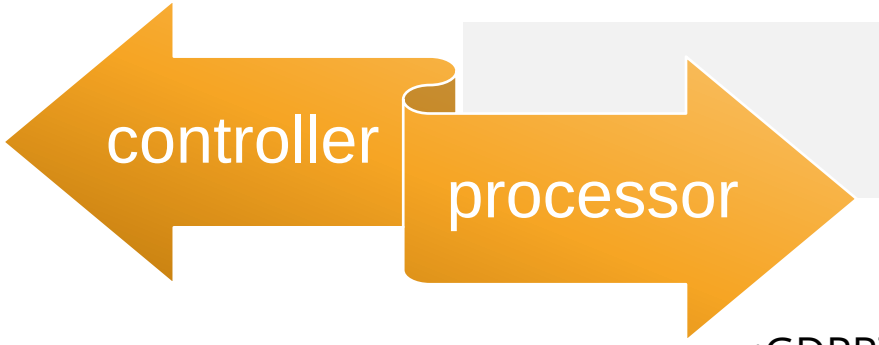
חוק הגנת הפרטיות

- מחזיק
  - גורם חיצוני לבעל השליטה המעבד בעבורו מידע [אישי]
- מונחים אחרים:
  - "גורם חיצוני" לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע (תקנות אבט"מ)
  - "מקבל המידע" (תקנות העברת מידע לחו"ל)

AYR

חשיבות הסכמי עיבוד מידע

- בתקנה 15 לתקנות אבט"מ הייתה חובה על בעל המאגר שיהיה הסכם שמסדיר את העיבוד
- תיקון 13 מטיל אחריות ישירה על המחזיק לקבל הרשאה:
  - "8(ג). לא יעבד אדם מידע אישי ממאגר מידע ללא הרשאה מאת בעל השליטה במאגר המידע או בחריגה מהרשאה כאמור"
  - "23נה. המעבד מידע אישי ממאגר מידע בלא הרשאה מאת בעל השליטה במאגר המידע, בניגוד להוראות סעיף 8(ג), דינו - מאסר שלוש שנים"
- האינטרס עבר לצד המחזיק
  - הגדרת עיבוד / שימוש מאוד רחבה
    - ההסכם צריך לכסות את כל סוגי השימושים



איך מבחינים

- מיהו בעל השליטה / controller
  - מי שולט על המידע? את מי משרת המידע? מי קובע את המטרות? [GDPR: מי קובע את האמצעים העיקריים]
- מה עושה המחזיק / processor
  - האם נותן שירות של עיבוד מידע או שירות אחר הכרוך בעיבוד מידע?
    - לגבי עיבוד המידע, האם החלטות המחזיק הן Essential vs. Non-essential
    - יכולת החלטה סופית של ה Controller, גם אם ה Processor קובע את תנאי השירות
- לפעמים הבחינה תוביל למסקנה ששני הצדדים הם Controller
  - Joint Controllers
- לפעמים יש כמה תפקידים בו-זמנית
- לפעמים התפקיד משתנה בהתקשרות

AYR

בעל שליטה או מחזיק?

- רשת פיצריות
  - שמקבלת הזמנות באפליקציה שלה
  - שמקבלת הזמנות באפליקציה כללית כמו Wolt (או הזמנת מונית באפליקציה כמו Gett)
    - מה תפקיד האפליקציה ומה תפקיד המסעדה?
    - האם הניתוח משתנה כשמדובר בחשבון תאגידי?
- שירות חשבות שכר
- ספק שירות ענן, ספק תקשורת
  - מה תפקידו כלפי צרכן ומה כלפי עובד בחברה שמשתמשת בשירות
  - שימוש במידע למטרות התחשבנות, שיפור השירות, הגנת סייבר, ציות לחוק
- בנק, חברת תעופה, חברת ביטוח
  - האם הניתוח משתנה אם הטיסה במסגרת העבודה? הבנק של המעסיק מעביר משכורת לעובד?
- עורך דין, רופא
  - פרטי, ומטעם המעסיק

הסכמה לעיבוד מידע

- פרק א' –
  - סעיף 2(9): פגיעה בפרטיות היא אחת מאלה... שימוש בידיעה על **ענייניו הפרטיים** [ולא: מידע אישי] של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה.
    - ס' 1 : "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו"
- פרק ב' –
  - יידוע באיסוף ישיר (סעיף 11)
  - פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע תלווה בהודעה שיצויינו בה:
    - חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו
    - השלכות אי מסירה
    - מטרות ונעברים
    - זכויות עיון ותיקון
    - זהות בעל השליטה

AYR

הסכמה

- לפי הרשות, הבסיסים החוקיים לעיבוד הם הסכמה והסמכה
  - אבל האם כל עיבוד מחייב "בסיס" בישראל?
    - הסכמה נדרשת ל"פגיעה בפרטיות"
      - האם כל עיבוד פוגע בפרטיות?
      - מה לגבי עיבוד פוגע בפרטיות אבל מוצדק (חלה הגנה, למשל לפרסום עיתונאי)?

מה זה "בסיסים חוקיים"?

- תפישה של ה GDPR – כל עיבוד חייב בסיס חוקי
  - בלי בסיס - העיבוד אסור
- יש ב GDPR שישה בסיסים חוקיים לעיבוד
  - נדרש לביצוע חוזה
  - נדרש לקיום חובה חוקית
  - אינטרס חיוני של נושא המידע או אדם אחר
  - אינטרס לגיטימי של בעל השליטה
  - הסכמה
- רק בסיס אחד מהשישה הוא "הסכמה"
  - בכל שאר הבסיסים אין צורך בהסכמה לעיבוד
  - כל בסיסי העיבוד בעלי משקל שווה
    - הסכמה לא בסיס "יותר טוב"

AYR

הסכמה בישראל ובאירופה

- ס' 3: "הסכמה" – הסכמה מדעת, במפורש או מכללא
  - הרשות: עדיף מפורש, עדיף במעשה, עדיף לתת זכות חזרה, עדיף מרצון חופשי
- GDPR הסכמה חייבת להיות:
  - מפורשת וחד משמעית
  - נפרדת מעניינים אחרים
  - מרצון חופשי
    - אי אפשר להתנות את עצם קבלת השירות בהסכמה
  - זכות מוחלטת לחזור בך מהסכמה
  - איזה עיבוד ימשיך במקרה של משיכת הסכמה
    - ומה יהיה בסיס העיבוד שיחול במקרה כזה

AYR

אבל...

- בסיס ההסכמה ב GDPR **לא** משמש כבסיס לעיבוד נדרש לצורך קיום חוזה, לעמידה בהוראות החוק, לאבטחת מידע...
  - כי יש מבחר של בסיסי עיבוד אחרים עדיפים
  - כי הוא תלוי לחלוטין ברצון החופשי של האדם
- לא אמור להיות דומה בשום צורה להסכמה בחוק הגנת הפרטיות
  - תזכורת: כל בסיסי העיבוד שווים
    - בישראל – עדיף שהסכמה תהיה כמה שיותר חזקה
    - באירופה – הסכמה צריכה תמיד להיות חזקה – אבל יש חמישה בסיסי עיבוד שלא מצריכים הסכמה בכלל

הסכמה ובינה מלאכותית

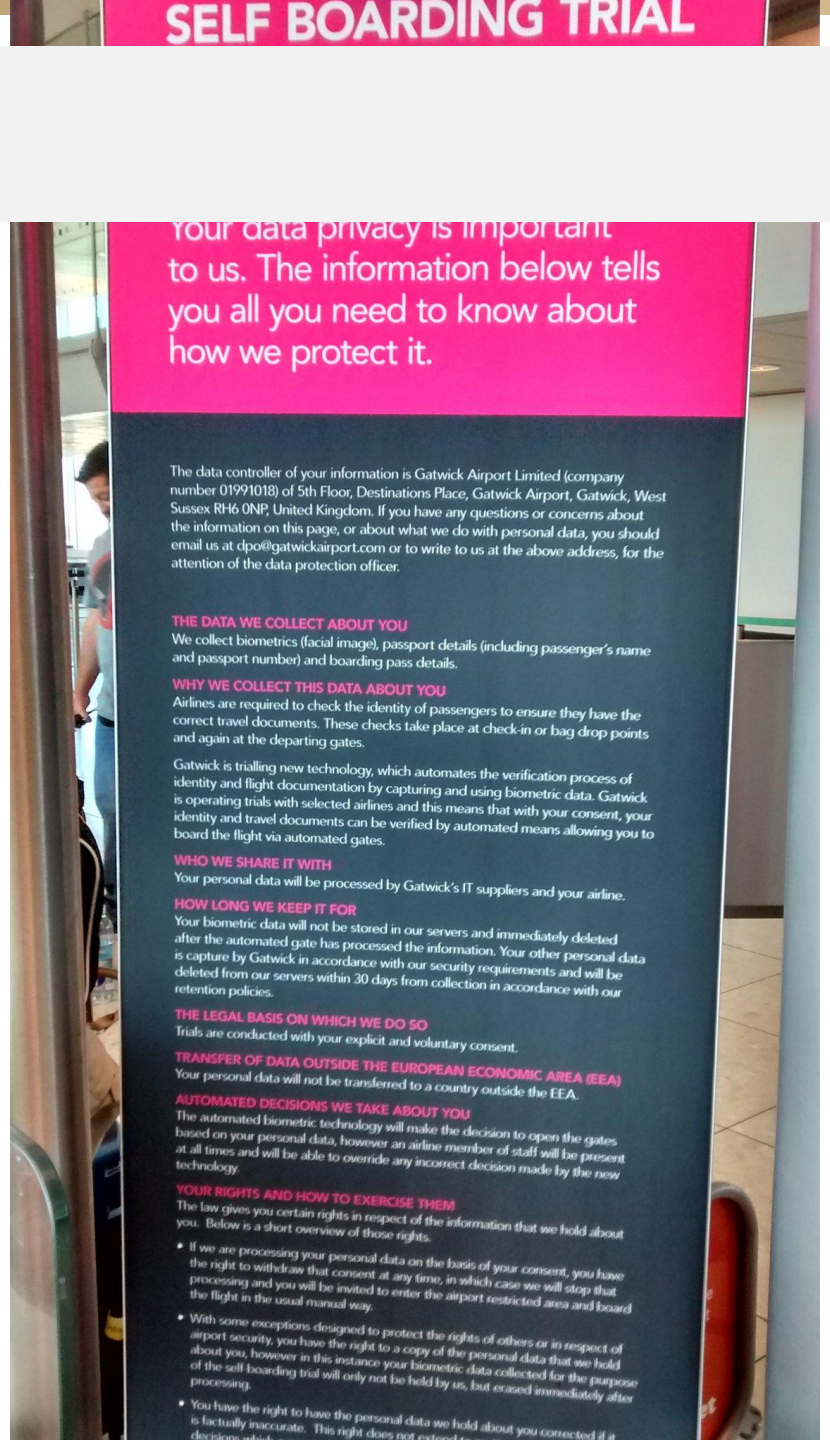
- הבסיסים החוקיים האפשריים לעיבוד לאימון מודלים:
  - אינטרס לגיטימי (לפיתוח ושימוש ב AI)
  - אינטרס חיוני (למנוע הטיה ואפליה במודלים)
  - הסכמה
- ישראל
  - הסכמה?
    - אז איך עובד מנוע חיפוש?
    - הגנות?
      - מוטלת על הפוגע חובה חוקית, מוסרית, חברתית או מקצועית לעשותה
      - הפגיעה נעשתה לשם הגנה על ענין אישי כשר של הפוגע
      - מה זה "אישי"?

יידוע לנושאי המידע

- שקיפות כלפי נושאי המידע נדרשת לפי...
  - ס' 11
  - תקנות הגישור
    - התקנות חלות על כל המידע באותו "מאגר", גם מידע אישי "ישראלי"
- יש עיצומים משמעותיים על הפרה של חובת היידוע
  - מה עושים לגבי התכתבות במייל, שיחת טלפון
  - איך מיידעים צדדים עקיפים?
  - לא לשכוח שהגדרת מידע אישי הורחבה מאוד

AYR

AYR
עמר רייטר ז'אן שוכטוביץ ושות'


SELF BOARDING TRIAL
to us. The information below tells
you all you need to know about
how we protect it.
The data controller of your information is Gatwick Airport Limited (company number 01991018) of 5th Floor, Destinations Place, Gatwick Airport, Gatwick, West Sussex RH6 0NP, United Kingdom. If you have any questions or concerns about the information on this page, or about what we do with personal data, you should email us at dpo@gatwickairport.com or to write to us at the above address, for the attention of the data protection officer.
THE DATA WE COLLECT ABOUT YOU
We collect biometrics (facial image), passport details (including passenger's name and passport number) and boarding pass details.
WHY WE COLLECT THIS DATA ABOUT YOU
Airlines are required to check the identity of passengers to ensure they have the correct travel documents. These checks take place at check-in or bag drop points and again at the departing gates.
Gatwick is trialling new technology, which automates the verification process of identity and flight documentation by capturing and using biometric data. Gatwick is operating trials with selected airlines and this means that with your consent, your identity and travel documents can be verified by automated means allowing you to board the flight via automated gates.
WHO WE SHARE IT WITH
Your personal data will be processed by Gatwick's IT suppliers and your airline.
HOW LONG WE KEEP IT FOR
Your biometric data will not be stored in our servers and immediately deleted after the automated gate has processed the information. Your other personal data is capture by Gatwick in accordance with our security requirements and will be deleted from our servers within 30 days from collection in accordance with our retention policies.
THE LEGAL BASIS ON WHICH WE DO SO
Trials are conducted with your explicit and voluntary consent.
TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)
Your personal data will not be transferred to a country outside the EEA.
AUTOMATED DECISIONS WE TAKE ABOUT YOU
The automated biometric technology will make the decision to open the gates based on your personal data, however an airline member of staff will be present at all times and will be able to override any incorrect decision made by the new technology.
YOUR RIGHTS AND HOW TO EXERCISE THEM
The law gives you certain rights in respect of the information that we hold about you. Below is a short overview of those rights.
• If we are processing your personal data on the basis of your consent, you have the right to withdraw that consent at any time, in which case we will stop that processing and you will be invited to enter the airport restricted area and board the flight in the usual manual way.
• With some exceptions designed to protect the rights of others or in respect of airport security, you have the right to a copy of the personal data that we hold about you, however in this instance your biometric data collected for the purpose of the self boarding trial will only not be held by us, but erased immediately after processing.
• You have the right to have the personal data we hold about you connected if it is factually inaccurate. This right does not extend

Sussex RH6 0NP, United Kingdom. If you have any questions or concerns about the information on this page, or about what we do with personal data, you should email us at dpo@gatwickairport.com or to write to us at the above address, for the attention of the data protection officer.

THE DATA WE COLLECT ABOUT YOU

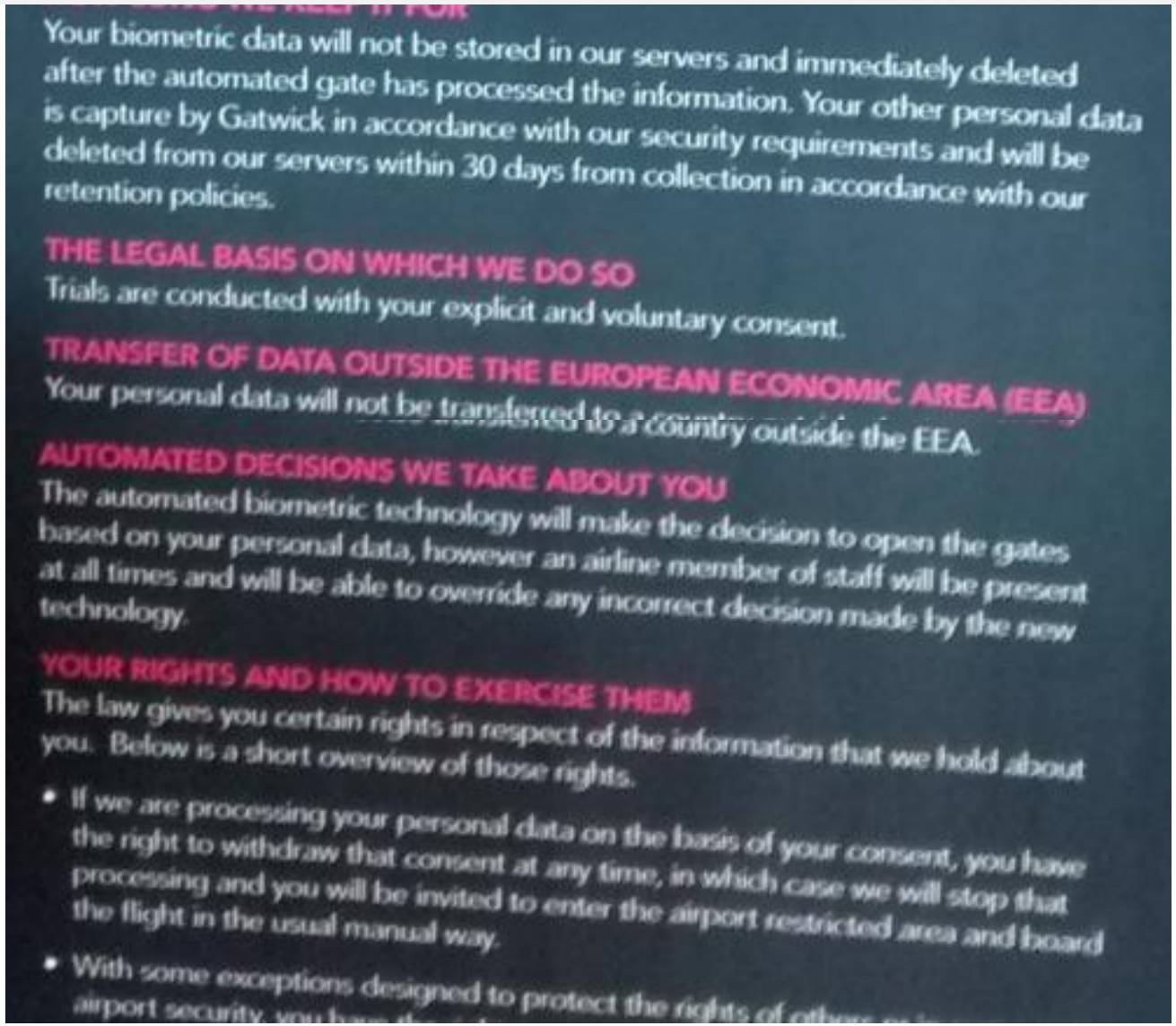
We collect biometrics (facial image), passport details (including passenger's name and passport number) and boarding pass details.

WHY WE COLLECT THIS DATA ABOUT YOU

Airlines are required to check the identity of passengers to ensure they have the correct travel documents. These checks take place at check-in or bag drop points and again at the departing gates.

Gatwick is trialling new technology, which automates the verification process of identity and flight documentation by capturing and using biometric data. Gatwick is operating trials with selected airlines and this means that with your consent, your identity and travel documents can be verified by automated means allowing you to board the flight via automated gates.

AYR



Your biometric data will not be stored in our servers and immediately deleted after the automated gate has processed the information. Your other personal data is capture by Gatwick in accordance with our security requirements and will be deleted from our servers within 30 days from collection in accordance with our retention policies.

THE LEGAL BASIS ON WHICH WE DO SO

Trials are conducted with your explicit and voluntary consent.

TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

Your personal data will not be transferred to a country outside the EEA.

AUTOMATED DECISIONS WE TAKE ABOUT YOU

The automated biometric technology will make the decision to open the gates based on your personal data, however an airline member of staff will be present at all times and will be able to override any incorrect decision made by the new technology.

YOUR RIGHTS AND HOW TO EXERCISE THEM

The law gives you certain rights in respect of the information that we hold about you. Below is a short overview of those rights.

- If we are processing your personal data on the basis of your consent, you have the right to withdraw that consent at any time, in which case we will stop that processing and you will be invited to enter the airport restricted area and board the flight in the usual manual way.
- With some exceptions designed to protect the rights of others or

מתוך אתר Aviva insurance
https://www.aviva.co.uk/

Commercial Insurance

Liability insurance

Business vehicle and van insurance

Property insurance

Other insurance for companies and sole traders

View Commercial Insurance Privacy Policy

Motor Insurance

Car insurance

Multi Car insurance

Van insurance

Breakdown cover

View Motor Insurance Privacy Policy

Home Insurance

Home insurance

Buildings insurance

Contents insurance

Tenants and renters insurance

Landlords insurance

View Home Insurance Privacy Policy

Travel Insurance

Travel insurance

View Travel Insurance Privacy Policy

Personal Accident Insurance

Accidental Death Insurance

Accidental Permanent Injury Insurance

Family Personal Accident Plan

Hospital Cash Plan

View Personal Accident Insurance Privacy Policy

Health Insurance

Private medical insurance

Speedy Diagnostics

View Health Insurance Privacy Policy

AYR

Individual Protection Insurance

Life insurance

Over 50 life insurance

Free Parent Life Cover

Income protection insurance

Critical illness cover

View Individual Protection Insurance Privacy Policy

Group Protection Insurance

The following policies provided by your employer:

Life insurance

Income protection insurance

Critical illness cover

View Group Protection Insurance Privacy Policy

Retirement

Pension

Pension annuity

Pension transfers

Income drawdown

Lifetime Care

Equity release

View Retirement Privacy Policy

Investments

Stocks & Shares ISA

Investment Account

Investment Bonds

Aviva Financial Advice

View Investments Privacy Policy

Aviva Save

Aviva Save

View Aviva Save Privacy Policy

Other Insurance

Creditor Insurance

Gadget Insurance

Valuables Insurance

View Other Insurance Privacy Policy

If you are not an Aviva customer or beneficiary (or a prospective customer or beneficiary), please select the “other parties” privacy policy below.

Other parties

Third Party Claimants

Witnesses

Executors

Trustees

Brokers and other appointed representatives

GPs and health professionals

Legal advisers

Experts and other professionals

View Other Parties Privacy Policy

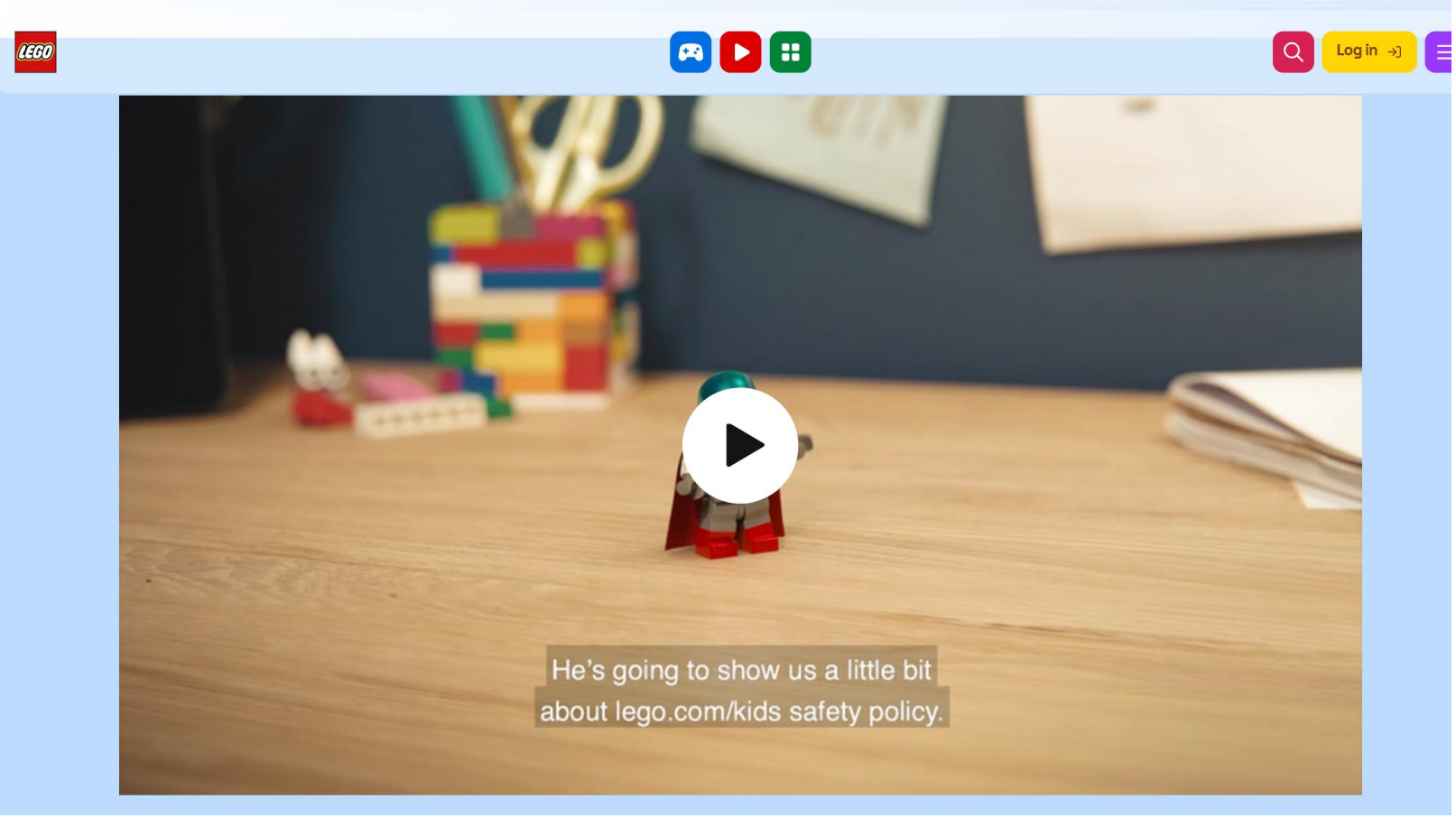
AYR

"מדעת" לקהל צעיר

- https://kids.lego.com/en-gb/legal/privacy-policy

Now some serious stuff

Learn about our policies on kids.LEGO.com



סעיפים טיפוסיים

- "החברה מכבדת את פרטיותם של לקוחותיה"
  - האם המשך המדיניות מראה שהחברה מכבדת את הפרטיות?
  - מה לגבי נושאי מידע שאינם לקוחות?
    - צדדי ג' במצב הכי חשוף, בלי מדיניות, בלי להיות לקוחות
- "המשתמש מאשר ומסכים כי כל הפרטים נמסרו על ידו מתוך הסכמה, בחירה ורצון חופשי"
  - זה שכתבנו "מתוך הסכמה מרצון חופשי" לא אומר שיש הסכמה או רצון חופשי
- "כל המידע הוא קניינה של החברה, והמשתמש מסכים ומאשר כי הדבר לא יחשב כפגיעה בפרטיות ומוותר בזאת על כל טענה בגין שימוש במידע כאמור"
  - אי אפשר לוותר על זכות לפרטיות בצורה כזו (אפילו לא בארץ)
  - קניין במידע אישי ≠ מנהג בעלים
- "במקרה של אי הסכמה הסר את האפליקציה"
  - האם מידע כבר נאסף (ועל הדרך הודינו שצריך הסכמה לדעתנו)
- "המידע ישמש לכל מטרה חוקית לפי קביעת החברה מעת לעת"
  - המטרות לא מוגדרות מראש וניתנות לשינוי – יסוד "מדעת"

"מאגר"

- "אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי..."
  - אותו המידע (ומידע מסוגים שונים, עובדים, לקוחות) נמצא בארגון בהרבה מקומות:
    - מערכת תיוק
    - דואר אלקטרוני
    - האם כל המידע האישי בארגון נמצא ב"מאגר" מוגדר?
  - אז כמה מאגרים יש לנו?
- הקביעה משפיעה על:
  - מסמך הגדרות המאגר
  - צורך במינוי ממונה אבטחה
  - ספירה לצורך סיווג המאגר
  - ספירה לצורך דיווח לרשות
  - גובה העיצומים (בעיקר במאגרים שהעיצום הוא מכפלה של נושאי המידע)
  - דיווח על אירוע אבטחה
  - תחולת תקנות העברת מידע מה EEA

AYR

מידע רגיש

תיקון 13

- מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישותו ועל נטייתו המינית;
- מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי;
- מידע גנטי;
- מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב;
- מידע אישי על מוצאו של אדם;
- מידע אישי על אודות עברו הפלילי של אדם;
- מידע אישי על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם או השקפת עולמו;
- מידע אישי שהוא הערכת אישיות שנערכה מטעם גורם מקצועי;
- מידע אישי שהוא נתוני מיקום ונתוני תעבורה על ידי ספק מורשה (לפי החסד"פ)... ונתונים על אודות מיקומו של אדם שיש בהם כדי ללמד על מידע אישי אחר;
- מידע אישי על נתוני שכר של אדם ועל פעילותו הפיננסית;
- מידע אישי שחלה עליו חובת סודיות שנקבעה בדין;

תקנות אבטחת מידע

- מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד;
- מידע רפואי או מידע על מצבו הנפשי של אדם;
- מידע גנטי;
- מידע על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם;
- מידע על אודות עברו הפלילי של אדם;
- נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007
- מידע ביומטרי
- מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם
- הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע כאמור לעיל או על אישיותו של אדם, אמונתו או דעותיו

מידע רגיש: חובת דיווח לרשם ורמת האבטחה

- דיווח לרשות לפי חוק הגנת הפרטיות:
  - "עלה מספר בני האדם שיש על אודותיהם מידע בעל רגישות מיוחדת במאגר מידע שאינו מאגר חייב ברישום... על 100,000, יודיע בעל השליטה במאגר המידע לרשות"
    - שאלת צד: איך סופרים אנשים במידע לא מובנה?
- רמת אבטחה גבוהה לפי תקנות אבטחת מידע:
  - מאגר הכולל מידע רגיש [לפי התקנות] +
  - שיש בו מידע [כלשהו?] על אודות 100,000 אנשים ומעלה
    - שאלת צד: איך סופרים אנשים במידע לא מובנה?
  - או שיש מעל 100 מורשי גישה
  - איך סופרים "מורשי גישה"?
    - יחיד אשר יש לו גישה לאחד מאלה על פי הרשאתו של בעל המאגר או המחזיק:
      - מידע מהמאגר
        - לא כולל לקוח שניגש למידע על עצמו
      - מערכות המאגר
      - מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו
      - מורשים: כוללים IT

מידע עודף בתקנות אבטחת מידע

- 2(ג). בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.
  - אין חובת מחיקה מפורשת
  - אבל יש חובה לתעד את הבדיקה לאור תקנה 19(ב)
    - תיעוד שיש מידע לא נדרש – הוכחה אפשרית לרשלנות במקרה של אירוע אבטחה

מחיקת מידע בתקנות הגישור (תקנה 4)

- "4. בעל מאגר מידע יפעיל מנגנון ארגוני, טכנולוגי או אחר, שמטרתו להבטיח כי במאגר המידע לא מוחזק מידע שאינו נחוץ עוד למטרה שלשמה נאסף או הוחזק או למטרה אחרת שלשמה מותר להחזיקו לפי כל דין ...**ימחק** את המידע שאינו נחוץ במועד המוקדם האפשרי בנסיבות העניין."
- מנגנון
  - ארגוני
    - לא פעם בשנה כמו ב 2(ג), אלא רציף
  - טכנולוגי

מחיקת מידע בתקנות הגישור (תקנה 3)

- 3. בעל מאגר מידע **ימחק** מידע לבקשתו הכתובה של נושא המידע בהתקיים אחד מאלה:
  - המידע נוצר, נתקבל, נצבר או נאסף בניגוד להוראות כל דין, או שהמשך השימוש בו מנוגד להוראות דין
  - המידע אינו נחוץ עוד למטרות שלשמן נוצר, נתקבל, נצבר או נאסף
- תיאורטית מי שעובד נכון בתקנה 4 לא יגיע לתקנה 3
- בעל מאגר מידע יודיע בכתב לנושא המידע על החלטתו בבקשה, במועד המוקדם האפשרי בנסיבות העניין
  - אין חובת הנמקה ("...על החלטתו...") אבל...

חריגים למחיקה בתקנות הגישור

- נותנים אינדיקציה גם לתקנה 2(ג) לתקנות אבטחת מידע
- התממה
  - "יבצע פעולות המבטיחות שלא יתאפשר, באמצעים סבירים, לזהות את נושא המידע"
- צידוקים
  - אם השימוש במידע הוא לצורך אחד מאלה, וזאת **בהיקף הנחוץ והמידתי** לאותו צורך
    - מימוש חופש הביטוי או זכות הציבור לדעת, הסכם בין-לאומי שישראל צד לו
    - ניהול הליך משפטי או גביית חובות
    - מניעת הונאה, גניבה, או מניעת פעולות אחרות שעלולות להשפיע על דיוק המידע או מהימנותו
    - להגנה על עניין ציבורי, **לרבות** למטרות ארכוב, מחקר מדעי או מחקר סטטיסטי...
  - GDPR 17(3)(d): for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes...

AYR

אייל שגיא

eyals@ayr.co.il

www.ayr.co.il

AYR

עמר רייטר ז'אן שוכטוביץ ושות'

המצגת אינה תחליף לייעוץ משפטי