**סיכום פגישה בנושא compliance עם אירית 24.11.24**

Compliance- הגנה על המידע, והגנה על חוקי הפרטיות

GDPR – איחוד אירופאי, החוק הראשון שעבר בנושא הגנה על הפרטיות

בארץ החוק להגנת הפרטיות עוקב אחר ה-GDPR

בקליפורניה – CCPA

ישנם מס' כללים שעלינו לעמוד בהם כשאנו אוספים מידע, GDPR מגן על תושבי האיחוד האירופאי.

1. consent – עלינו לידע את הלקוח שאנו אופים מידע ואיזה מידע אנו אוספים עליו, ורק אם היוזר מאשר מותר לנו לאסוף עליו מידע. ההסכמה חייבת להיות explicit
2. Transparency – שקיפות, אנו חייבים ליידע את הלקוח איזה מידע אנו אוספים עליו.
3. Data minimizing – לאסוף אך ורק מידע נדרש לצורך שירות המטרה שבשמה אנו אוספים מידע.
4. Right to access/remove- לכל אדם שנאסף עליו מידע, יש את האפשרות לגשת לאותו מידע, לעדכנו או למחוק אותו. (למחוק יכול להיות שהאדם יאלץ להגיש בקשה ואנו נמחק ונוכיח לו שהמידע עליו נמחק).
5. Retention – כמה זמן צריך לשמור את המידע?

צריך לפרט איה סוג קוקיז נאסוף, לדוגמא – כתובת IP, לכמה זמן הקוקיז יישארו, חייבים לתת אפשרות ליוזר לבחור אם לאשר או לדחות קוקיז ואם לאפשר אז מה לאפשר (הכל או חלק).

איך מתייחסים לprivacy by design

צריך לפרט איזה הגנות אבטחתיות אנו נשים כדי לשמור על המידע. (לדוגמא מערכת DLP במערכת גדולה שאוספת הרבה מידע).

חייבים מסמך privacy policy ולציין שם איך המערכת בנויה כדי לשמור את המידע של היוזרים מוגן.