

Kamerák, compliance és az azonnali tájékoztatás kockázata – mit üzen a Bíróság a vállalatoknak a testkamerák használatáról?

Az Európai Unió Bíróságának friss, 2025. december 18-án hozott ítélete egy látszólag szűk, közlekedési vállalatokat érintő adatvédelmi kérdésen keresztül valójában sokkal szélesebb körű üzenetet hordoz minden olyan vállalkozásnak, amely megfigyelési technológiákat, különösen kamerarendszereket alkalmaz üzleti működése során. A döntés világossá teszi, hogy a GDPR tájékoztatási kötelezettségeinek értelmezése a gyakorlatban sokkal szigorúbb, mint ahogyan azt számos adatkezelő eddig feltételezte, és hogy a „technológiai semlegesség” nem jelent compliance-kockázatmentességet.

Az Európai Unió Bíróságának friss, 2025. december 18-án hozott ítélete egy látszólag szűk, közlekedési vállalatokat érintő adatvédelmi kérdésen keresztül valójában sokkal szélesebb körű üzenetet hordoz minden olyan vállalkozásnak, amely megfigyelési technológiákat, különösen kamerarendszereket alkalmaz üzleti működése során. A döntés világossá teszi, hogy a GDPR tájékoztatási kötelezettségeinek értelmezése a gyakorlatban sokkal szigorúbb, mint ahogyan azt számos adatkezelő eddig feltételezte, és hogy a „technológiai semlegesség” nem jelent compliance-kockázatmentességet.

Az ügy középpontjában egy stockholmi közlekedési vállalat gyakorlata állt, amely jegyellenőrei számára testkamerákat biztosított, és ezek segítségével rögzítette az ellenőrzések során történeteket. A tagállami adatvédelmi hatóság bírságot szabott ki arra hivatkozva, hogy az érintett utasok nem kaptak megfelelő és időben nyújtott tájékoztatást a személyes adataik kezeléséről. A vállalat védekezése szerint a kamerafelvételek révén kezelt adatok nem közvetlenül az érintettektől származtak, ezért nem a GDPR 13. cikke, hanem az enyhébb követelményeket támaztó 14. cikk volt alkalmazandó.

A Bíróság ezt az érvelést egyértelműen elutasította, és kimondta, hogy a testkamerával rögzített képfelvétel tipikusan közvetlen adatgyűjtésnek minősül. Ennek megállapításához nem szükséges, hogy az érintett aktívan adatot szolgáltatson, vagy akár tudatosan közreműködjön az adatkezelésben. Már az is elegendő, hogy az adatkezelő az érintett megfigyelésével jut személyes adatokhoz. Ez az értelmezés lényegében minden olyan üzleti szituációra kiterjeszthető, ahol a vállalat kamerák, szenzorok vagy hasonló technológiák útján „észleli” az érintetteket.

A döntés egyik legfontosabb gyakorlati következménye az, hogy ilyen esetekben a tájékoztatást azonnal meg kell adni. A Bíróság ugyanakkor elfogadja az úgynevezett többrétegű tájékoztatási modellt, amely a nagy forgalmú, dinamikus környezetben működő szervezetek számára különösen releváns. Eszerint a leginkább lényeges információk – így az adatkezelés ténye, célja és az adatkezelő kiléte – akár egy jól látható figyelmeztető jelzésen is megjelenhetnek, míg a részletes adatvédelmi információk egy könnyen hozzáférhető csatornán, például QR-kódon, weboldalon vagy fizikai tájékoztatón keresztül biztosíthatók.

Üzleti szempontból az ítélet túlmutat a közösségi közlekedés világán. Érinti a biztonsági szolgáltatásokat, a kiskereskedelmi szektort, a logisztikát, a rendezvényszervezést, sőt a munkahelyi környezetet is, ahol testkamerák, mobil kamerák vagy viselhető technológiák egyre gyakrabban jelennek meg. A Bíróság üzenete egyértelmű: az ilyen eszközök alkalmazása nem csupán technikai vagy operatív

kérdés, hanem az adatvédelmi governance központi eleme, amelynek hiányosságai közvetlen pénzügyi és reputációs kockázatot hordoznak.

A döntés egyben azt is jelzi, hogy a hatóságok és a bíróságok a jövőben várhatóan kevésbé lesznek elnézőek azokkal a megoldásokkal szemben, amelyek a tájékoztatási kötelezettséget pusztán formális, utólagos vagy nehezen hozzáférhető dokumentációval kívánják „kipipálni”. A compliance itt nem dokumentumgyártást, hanem az érintetti minőség tényleges átgondolását jelenti.

Összességében az ítélet egy világos stratégiai üzenetet hordoz a vállalatvezetők és jogi tanácsadók számára. A megfigyelési technológiák használata során nem az a kérdés, hogy keletkezik-e adatvédelmi kötelezettség, hanem az, hogy az adatkezelő képes-e azt az üzleti folyamatokba integrált, azonnali és érthető módon teljesíteni. Aki ezt alábecsüli, az nem csupán egy GDPR-bírságot, hanem a fogyasztói bizalom elvesztését is kockáztatja.