Mauritiusi deklaráció – 36. Nemzetközi Adatvédelmi Konferencia

Az okos eszközök használata mindennapivá vált. Egyre több készülék kapcsolódik az internethez és képes arra, hogy kommunikáljon egymással, sokszor anélkül, hogy a felhasználó ennek tudatában lenne. Ezek a készülékek életünket sokkal könnyebbé, egyszerűbbé tehetik, akár például az egészségügy, a közlekedés, energia területén, így tehát ezek az internethez kapcsolódó eszközök megváltoztathatják szokásainkat.
Az okos eszközök kiszolgáltatott helyzetbe is hozhatják tulajdonosukat, ugyanis érzékelőik segítségével felfedhetik a felhasználó egyes személyes ügyeit és szokásait.

Az önmeghatározás elidegeníthetetlen joga minden embernek. A személyiség fejlődése nem szabad, hogy az üzleti világ és a kormány által szerzett információktól legyen meghatározott. Az okos eszközök elterjedése csak fokozza a kockázatát annak, hogy ez megtörténjen. Az összegyűlt adatvédelemi biztosok ezért vitatták meg az okos eszközök által kínált lehetőségeket, és annak következményeit 2014. október 13-án és 14-én, Mauritiuson, a Balaclava városban tartott 36. Nemzetközi Adatvédelmi Konferencia során.

A magánszektort és az akadémiai szférát képviselő négy előadó tartott előadást a biztosoknak azokról a pozitív változásokról, ill. kockázatokról, amelyet az okos eszközök hozhatnak mindennapjainkba. Az előadók azt is megállapították, milyen intézkedéseket kell tenni annak érdekében, hogy a személyes adataink és magánéletünk védelme biztosított legyen.

A Konferencia alapján a következő észrevételek, és következtetések vonhatóak le:

- Sokféle, jó minőségű, és nagyfokú érzékenységgel rendelkező okos eszköz van. Ez azt jelenti, hogy a levonható következtetések sokkal nagyobbak, és érzékenyebbek, így az egyedi azonosíthatóság valószínűbbé válik. Figyelembe véve, hogy az egyedi azonosíthatóság és a nagy mennyiségű adatok védelme egy már jelentős kihívásnak számít, világos, hogy az okos eszközöktől származó nagy mennyiségű adat, a kihívást sokszor még nagyobbá teszi. Ezért az ilyen adatot olyannak kell tekinteni, és úgy kell kezelni, mint személyes adatot.
- Még ha sok vállalatnak ismeretlen is mostanáig ez az üzleti modell, az biztos, hogy az okos eszközök értéke nem csak önmagában a készülékben rejlik. A gazdasági megtérülés az új szolgáltatásokban rejlik, melyek az okos eszközökhöz és azok adataihoz kapcsolódnak.
- Napjaink emberei tudatában vannak a ténynek, hogy ez a kapcsolat mindenütt jelen van. Ezt talán a fiatalabb generációkra érvényes a leginkább, akiknek elképzelhetetlen a világ internet kapcsolat nélkül. Bár nem kizárólag nekik kellene aggódniuk, hogy adataik védve vannak e vagy sem. Ez közös felelőssége a társadalom valamennyi szereplőjének, azért hogy a bizalom az internet rendszere iránt fennmaradjon. Ezért az átláthatóság a kulcs: azok, akik ilyen okos eszközöket kínálnak, tisztában kellene lenniük azzal, hogy milyen típusú adatot gyűjtenek, milyen célokra, és mennyi ideig tárolják azokat. Meg kell semmisítsék az adatösszefüggésekből „kitűnő" részeket, melyek esetleges meglepetésként érhetik az ügyfelet. Amikor valaki egy okos eszközt, alkalmazást vásárol, arról hiteles, megfelelő, és érthető információkkal kell ellátni. A hatályos adatvédelmi rendelkezések gyakran nem szolgáltatnak tiszta, és érthető módon információt, így ez alig tekinthető előzetes hozzájárulásnak. Az ilyen szolgáltatást nyújtó cégeknek eszmeváltásra van szükségük, hogy megbizonyosodhassanak róla: az adatvédelmi rendelkezések elsősorban arról szólnak, hogy megvédjék őket a bírósági eljárástól.
- Az adatkezelés abban a pillanatban elindul, mikor az adatot gyűjteni kezdik. Ahol az adatkezelést megkezdték, ott minden védőintézkedést az elejétől fogva alkalmazni kellene. Támogatjuk azon technológiai fejlesztéseket, amelyek kezdettől fogva új módszereket

támogatnak azzal a céllal, hogy az adatvédelem és a fogyasztók védelme egybeolvadhasson. A beépített adatvédelmet (*privacy by design*), és az alapértelmezett adatvédelmet (*privacy by default*) nem kellene tovább különlegesnek, speciálisnak tekinteni. Ezeknek a fejlődő technológiáknak kulcsfontosságú kell válniuk az értékesítésben.
- Az okos eszközök lényeges biztonsági kihívást jelentenek, mellyel foglalkozni kell. Egy egyszerű tűzfal már rég nem elegendő. Egy lehetséges útja annak, hogy a kockázat az egyének felé csökkenthető legyen: meg kell győződni arról, hogy az adatokat feldolgozza-e magától a készülék (helyi adatfeldolgozás). Ha ez nem lehetséges, a vállalatoknak teljes mértékben gondoskodniuk kell a titkosításról azért, hogy az adatok védve legyenek az illetéktelen beavatkozástól és/vagy a meghamisítástól.
- Az adatvédelmi hatóságok folytatni fogják az okos eszközök fejlődésének ellenőrzését. Magukra vállalják, hogy biztosítsák saját országaikban az adatvédelem, ill. annak törvényi szabályozásának, valamint a nemzetközileg elfogadott adatvédelmi elveknek betartását. Azon országokban ahol a törvény megsértését tapasztalják, ott szankciót fognak alkalmazni, amely történhet egyoldalú módon, vagy nemzetközi együttműködési eszközökön keresztül is.
- Figyelembe véve az okos eszközök fejlesztőit érő kihívásokat, az adatvédelmi hatóságoknak, az egyéneknek, és az összes szereplőnek egy erős, aktív és konstruktív vitában kellene részt venniük - bevonva az okos eszközök gyártóit és az abból származó nagy adatmennyiség kezelőket - hogy felhívják a figyelmet arra, hogy milyen döntéseket kell a jövőre nézve meghozni.