Az mHealth applikációk adatvédelmi kérdései

DR. HORVÁTH KATALIN

Az mHealth applikációk egyre elterjedtebbek, azonban egyre több jogi kérdést vetnek fel. Személyes adatokat és egészségügyi adatokat kezelő alkalmazásokról lévén szó, az adatvédelmi, adatbiztonsági kérdések egyre fontosabbak az ilyen appok fejlesztőinek és felhasználóinak. A cikk az mHealth applikációkkal kapcsolatos legfontosabb adatvédelmi kérdéseket járja körül, választ keresve arra is, hogyan alakul a szabályozás az Európai Unió új adatvédelmi rendeletének 2018-as hatályba lépésével.

Az mHealth applikációk elsősorban azok a mobiltechnológiák, amelyek az azokat használó felhasználók által megadott személyes adatokat, azon belül pedig különösen érzékeny egészséggel kapcsolatos adatokat gyűjtenek, kezelnek akár magán az azt futtató okoseszközön, akár valamilyen felhő alapú technológián keresztül tárolva, és amelyek alapvetően képesek ezeket az adatokat hozzáférhetővé tenni, megosztani a széles nyilvánossággal. Ebbe a körbe tartoznak a hordható, hordozható, beültethető eszközök és technológiák, amelyeket egyének használnak a saját egészségük, fittségi állapotuk monitorozására vagy egészségük kezelésére. Ezek a technológiák támogathatják pl. az orvosi ellátást (diagnózis és betegség kezelése), és lehetnek életmóddal kapcsolatos céljaik is (súlycsökkentés, egészséges diéta, dohányzásról való leszokás, fizikai erőnlét javítása). Ebbe az átfogó kategóriába tartoznak pl. a hordható fitnesszokoseszközök, viselhető érzékelők, vezeték nélküli adatátvitelt lehetővé tevő hálózatok, okostelefonok, közösségi média hálózatok.

Az mHealth alkalmazások egyszerre vagy külön-külön többféle célt is szolgálhatnak:[1]

- ***fiziológiai paraméterek monitorozása:*** mérés, rögzítés, riportolás, pl. szívritmus, vérnyomásadatok;
- ***aktivitás és viselkedés monitorozása:*** mozgási, fizikai és szociális aktivitás mérése, rögzítése, riportolása vagy pl. étkezési szokások figyelése;
- ***információhoz való hozzáférés:*** egészséggel kapcsolatos adatokhoz való hozzáférés biztosítása, pl. leletek letöltése, döntéstámogató eszközök, egészségügyi adatok feltöltése és eljuttatása az orvoshoz;
- ***távolról történő orvoslás (telemedicina):*** a beteg és az orvos közötti kommunikáció, pl. virtuális orvosi látogatás lebonyolítása.

A fent említett mHealth eszközök új lehetőséget jelentenek mind az egyének, mind pedig a közegészségügy és annak valamennyi résztvevője számára. Ezekkel az egészségügyi, fitnessz, sport és életmód mobilapplikációkkal, eszközökkel hatékonyabbá tehető a gyógyításban, betegellátásban az orvos-beteg kapcsolat, lehetővé válik az egészségi állapottal kapcsolatos adatok egy helyen történő tárolása. Ezen túlmenően a mobil egészségügyi technológiával javítható az egészségügyi ellátás színvonala, növelhető az egészségügyi szolgáltatásokhoz való hozzáférés, és nem utolsósorban csökkenthetők az egészségügyi költségek azáltal, hogy az egyének tudatosságát növeli az egészségmegőrzés területén, ösztönzi az egészséges életmódot, és fontos szerepet játszik a betegségek megelőzésében is.

DR. HORVÁTH KATALIN
Partner ügyvéd, Sár és Társai Ügyvédi Iroda, Budapest

A mobiltechnológiák elterjedése az egészségügyben a különböző orvosi és

gyógyszerészeti kutatás-fejlesztéseket is nagymértékben segítheti, hiszen ezekkel az mHealth technológiákkal tömegesen és könnyen gyűjthetők tudományos, kutatási, statisztikai célra adatok a célközönségtől, amelyek a kutatásokban is felhasználhatók.

Felhasználói oldalról is egyre nagyobb az igény az ilyen mobilalkalmazásokra, hiszen a közösségi média világában szocializálódott, mobil okoseszközökön felnőtt fiatal korosztály számára az a természetes, hogy nem csupán napi tevékenységükkel kapcsolatos információkat osztanak meg a világhálón, hanem fittségi állapottal, étrenddel, életmóddal kapcsolatos adatokat is, gondoljunk itt pl. a sport- és fitnesszapplikációk által mért testmozgási teljesítményekre, az ezekkel kapcsolatos okosórák, okoseszközök által mért egyéb adatokra: lokációra, távolságra, pulzusra, domborzati viszonyokra, elégetett kalóriára, lépésszámra, orvosi diagnózisokra, leletekre. Ráadásul ez a korosztály már nem azonnal az orvoshoz fordul, ha egészségügyi problémája merül fel, hanem először a közösségi média hálózatokon, speciális csoportokban, az interneten keres válaszokat és gyógymódokat, miközben jelentős mennyiségű egészségügyi és személyes adatot közöl magáról a gyors problémamegoldás reményében.

Az mHealth appok, közösségi médiafelületek azonban csak akkor segíthetnek a fenti előnyök kiaknázásában, ha az adataik biztonságába vetett bizalom, valamint az információs szimmetria az egyének és a szolgáltatójuk oldalán fennáll. Az mHealth appok nagyon sérülékenyek, tekintettel arra is, hogy érzékeny egészségügyi adatokat tárolnak, gyakran sajnos nem elégséges adatbiztonsági eszközök mellett és nem megfelelő tájékoztatást nyújtva a felhasználóiknak.

Az mHealth appok esetében ezért fokozottan kell ügyelni az adatvédelmi, adat- és információbiztonsági előírások megfelelő betartására.

MILYEN ADATOKAT KEZELHETNEK AZ MHEALTH APPOK?

Az mHealth alkalmazások egyrészt személyes adatokat, másrészt egészségügyi adatokat kezelhetnek a felhasználókról. A kétféle adattípus elkülönítése jogi szempontból releváns, mivel eltérő szabályok vonatkoznak mind a magyar, mind az uniós jogban a kétféle adattípus kezelésére. Az mHealth appok esetében ezért először arról kell meggyőződni, hogy melyik típusba tartoznak a gyűjtött, kezelt adatok.

Személyes adatnak a magyar szabályozás alapján[2] valamennyi, a felhasználóval kapcsolatba hozható adat minősül, így pl. a felhasználó neve, azonosító jele, lokációja, a fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző egy vagy több ismeret, valamint az adatból levonható, a felhasználóra vonatkozó következtetés.

Ezzel szemben egészségügyi adat a felhasználó testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátó hálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, azokat befolyásoló mindennemű adat (pl. magatartás, környezet, foglalkozás).[3] Ebbe a körbe tartoznak pl. a hordható vagy beültetett szenzorok, érzékelők által gyűjtött adatok (vérnyomás, pulzus, szívritmus, cukorszintmérő stb.), amelyekből az egészségügyi állapotra vonható le következtetés.

A kétféle adattípus elkülönítése nem mindig egyszerű, különösen az életmóddal kapcsolatos adatok esetében, amelyek egyszerű személyes adatként kezelendők akkor, ha nem kapcsolódnak az egyén egészségéhez. Egészségügyi, és nem puszta személyes adatot kezel pl. az az alkalmazás, amely az orvos által felírt gyógyszer bevételét ellenőrzi, nem kezel azonban ilyen adatot az az alkalmazás, amely lépésszámot rögzít, sportaktivitást mér. Ha viszont ezeket az adatokat egészségügyi kockázatok mérésére vagy előrejelzésére használják, vagy a felhasználó egészségi állapotának megállapításához tárolják, akkor felmerül az egészségügyi adatok kezelésének lehetősége is.[4]

Még szigorúbb szabályok vonatkoznak a biometrikus és genetikai adatok kezelésére, ezért ezt is szükséges vizsgálni az applikációk fejlesztésének folyamatában.

Akár személyes, akár egészségügyi, biometrikus vagy genetikai adatokat kezel az alkalmazás, mindenképpen szükséges az adatkezelés megkezdése előtt részletesen tájékoztatni a felhasználót a kezelt adatok pontos köréről.[5] Ez a szabály alkalmazandó a felhasználó által bevitt adatokra, vagyis pl. a regisztráció során megadott személyes adatokra (telefonszám, név, e-mail cím, lakcím stb.), az app által kért, további számításokhoz használt adatokra (pl. nem, születési dátum vagy életkor, testmagasság, testsúly, bevitt napi kalóriamennyiség).

Az mHealth alkalmazások azonban általában nem csupán azokat az adatokat kezelhetik, amelyeket a felhasználók visznek be közvetlenül az alkalmazásba, hanem az applikáció automatikusan is mér és tárol különböző értékeket: geolokációs adatokat, lépésszámot, sebességet, megtett távolságot, mért vérnyomást, szívritmust, pulzusszámot, amelyek körét szintén előzetesen közölni kell a felhasználóval, és az ilyen adatok egy része már egészségügyi adatnak minősül, amelyeket külön fel kell tüntetni. Ugyanez a szabály vonatkozik az alkalmazás által automatikusan gyűjtött adatokra is, amelyek általában az alkalmazással kapcsolatos viselkedési adatokat, használati szokásokat, GPS adatokat, az appot használó készülék jellemzőit, a használt operációs rendszert, mobilplatformot és egyebeket rögzítik és tárolják, amelyekről a felhasználónak szintén külön tájékoztatást kell kapnia. Lehetséges, hogy

ezek az automatikusan gyűjtött adatok önmagukban nem köthetők egy meghatározott személyhez, de az összességükből, összekapcsolásukból kirajzolódhat egy olyan profil, amelynek alapján az adott felhasználó beazonosítható, felismerhető, ez pedig már személyes adattá teszi az önmagukban annak nem minősülő adatokat.

A kezelhető (rögzíthető, gyűjthető, mérhető, tárolható) adatok körét, mennyiségét mind a magyar, mind az uniós jog szerint korlátozza az adatminimalizálás elve: csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas.[6] Gondosan meg kell tehát válogatni, hogy milyen adatokat gyűjtsön az alkalmazás, mivel csak azok az adatok kezelhetők, amelyek szigorúan véve szükségesek az app funkcionalitásának teljesítéséhez. Így pl. ha elegendő sávosan megadni az életkor adatát, akkor nem szükséges pontos születési dátumot kérni a felhasználótól.

MIRŐL ÉS HOGYAN KELL TÁJÉKOZTATNI A FELHASZNÁLÓT?

Az mHealth alkalmazást használók alapvető, Alaptörvényben rögzített joga, hogy követni és ellenőrizni tudják a velük kapcsolatos adatok kezelésének útját, vagyis azt, hogy az alkalmazásban ki, mikor, hol, milyen célra használja fel az ő személyes adataikat.[7] Ezt az általános szabályt váltja apropénzre Az információs önrendelkezési jogról és az információszabadságról szóló törvény (Infotv.), amikor meghatározza, hogyan és miről szükséges tájékoztatni a felhasználókat az adatkezeléssel kapcsolatban.[8] E tájékoztatás alapján képes ugyanis a felhasználó felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára. Az érintettek a megfelelő tájékoztatáson keresztül ismerhetik meg a személyes adataikra vonatkozó adatkezelést, illetve ezáltal érvényesülhet az információs önrendelkezési joguk. Megfelelő tájékoztatás hiányában az adatkezelő oldalán olyan „információs erőfölény" alakulhat ki, amelynek felhasználásával az érintett jogai, érdekei sérülhetnek.[9]

Az Infotv. fent hivatkozott szabályai alapján a tájékoztatásnak a következő kritériumoknak kell megfelelnie:

- az adatkezelés megkezdése előtt kell megtörténnie;
- részletes és egyértelmű tájékoztatást kell nyújtani egyszerű, zsargon nélküli, érthető, figyelemfelkeltő szövegben, amely a rendszeres/átlagos felhasználók számára érthető (vagyis nem megfelelő, ha az adatvédelmi szabályzat csak megismétli a jogszabály szövegét, a szabályzat lényege az, hogyan alkalmazza az mHealth app üzemeltetője önmagára a jogszabályokat);
- minden adatkezeléssel érintett tényre ki kell terjednie, vagyis teljesnek kell lennie, így tartalmaznia kell legalább az adatkezelés célját és jogalapját, az adatkezelésre és az adatfeldolgozásra jogosult személyét, az adatkezelés időtartamát, kik ismerhetik meg az adatokat; fel kell tüntetni azt is, hogy kinek és milyen célra továbbítják az adatokat, továbbá hogy az adatok feldolgozásához az applikáció üzemeltetője vesz-e igénybe adatfeldolgozót, és ha igen, milyen célra;
- tájékoztatni kell a felhasználót arról, hogy milyen jogai és jogorvoslati lehetőségei vannak az adatkezeléssel kapcsolatban;
- a tájékoztatásnak közvetlenül a felhasználóhoz kell eljutnia, közvetlenül elérhetőnek, jól láthatónak, feltűnőnek kell lennie (így pl. a nagyításra lehetőséget nem adó, nagyon kicsi betűméret sem alkalmazható);
- a tájékoztatásnak az átlagos felhasználók által beszélt nyelven kell megtörténnie, vagyis pl. ha egy magyar fejlesztésű alkalmazás külföldi felhasználók adatait is kezeli, nem elegendő pusztán magyarul közzétenni az adatvédelmi szabályzatot, szükség van ezen kívül legalább az angol nyelvű változatra is.[10]

HOGYAN KELL HOZZÁJÁRULÁST SZEREZNI AZ ADATKEZELÉSHEZ A FELHASZNÁLÓTÓL?

A magyar Infotv. szerint mHealth alkalmazásban is csak akkor kezelhető személyes adat, ha az adatkezeléshez a felhasználó hozzájárult, vagy az adatkezelést törvény közérdekből elrendeli. Az mHealth appok esetében, mivel azokat általában nem a közegészségügyi ellátásban, gyógyászati ellátórendszerben alkalmazzák, az adatkezelés szinte sosem jogszabályi engedélyen alapul. Ebből eredően ezeknek az alkalmazásoknak minden esetben hozzájárulást kell kérniük a felhasználóktól az adatkezeléshez. A hozzájárulásnak mindig meg kell felelnie a következő négy követelménynek:[11]

- a fentiekben említett előzetes tájékoztatáson kell alapulnia, mivel a hozzájárulást nem lehet megadottnak tekinteni olyan adatkezelés tekintetében, amelyről a felhasználót az alkalmazás üzemeltetője előzetesen nem tájékoztatta;
- önkéntesnek kell lennie, vagyis nem lehet szankciót alkalmazni, ha a felhasználó nem járul hozzá az adatkezeléshez, a hozzájárulás jelölőnégyzet nem lehet előre kipipálva, viszont lehet ajándékot, egyéb előnyt ígérni arra az esetre, ha a hozzájárulását a felhasználó megadja;
- határozottnak és félreérthetetlennek kell lennie: nem elegendő tehát annak biztosítása, hogy ha a felhasználónak nem tetszik, akkor tiltakozhat az adatkezelés ellen (opt-out), hanem hozzájárulást kell tartalmaznia, vagyis az opt-in elvet kell követnie;
- tényleges választási lehetőséget kell biztosítania a felhasználónak a hozzájárulás megadásánál a kezelt adatok körére és az adatkezelés céljára vonatkozóan.

Ha az mHealth alkalmazás nem pusztán életmódhoz kapcsolódó vagy egyéb személyes adatot, hanem egészségügyi adatot is kezel, még szigorúbb feltételeknek kell megfelelnie, amikor hozzájárulást kér a felhasználótól: kizárólag írásbeli hozzájárulás alapján kezelhetők ezek az adatok.[12]

Az egészségügyi adatokat gyűjtő, kezelő mHealth alkalmazások e jogi előírás miatt a magyar jogszabály alapján gyakorlati megvalósíthatóság szempontjából tulajdonképpen ellehetetlenülnek, hiszen az adatkezeléshez minden egyes felhasználótól írásbeli (pl. papír alapú vagy elektronikus aláírással ellátott) hozzájárulást kellene kérniük, ami kivitelezhetetlen a nagyszámú felhasználó miatt, és nem összeegyeztethető a mobilapplikációk lényegével: a bárhol, bárhonnan, azonnali elektronikus hozzáférhetőséggel. A nemzetközi és európai uniós viszonylatban is rendkívül szigorú magyar jogszabály nemcsak a magyar fejlesztésű alkalmazások üzemeltetőit köti, hanem minden olyan külföldi alkalmazás fejlesztőit/üzemeltetőit is, amely Magyarország területén folytat adatkezelést. Az mHealth alkalmazásokban az adatkezeléshez való hozzájárulás az esetek túlnyomó többségében nem felel meg, és technikai okokból nem is tud megfelelni e követelményeknek, vagyis elmondható, hogy a legtöbb, ma Magyarországon elérhető egészségügyi adatot kezelő mHealth applikáció nem tud jogszerűen működni.

MILYEN CÉLRA KEZELHETŐK AZ ADATOK?

Az mHealth alkalmazások – ugyanúgy, mint más mobilapplikációk – az általános adatkezelési elveknek megfelelően pontosan meg kell hogy határozzák mindazokat a célokat, amelyekre az adatokat kezelik.[13] A célok meghatározása kellően konkrét kell hogy legyen, így nem elfogadható olyan adatkezelési cél megjelölése, amely elfedi az adatok felhasználásának tényleges, valós indokát, célját. Az mHealth applikációk esetében pl. az egészségügyi adatok kezelésének célja egészségügyi jellegű, nem pedig gazdasági célt szolgál, így ha az üzemeltetők gazdasági, pl. marketing célra is kívánják használni a felhasználók egészségügyi adatait, akkor ezeket a gazdasági, marketing célokat külön fel kell tüntetniük az adatkezelésről szóló tájékoztatóban. Amennyiben az mHealth alkalmazás többféle adatot sokféle célra kezel, szükséges a kezelt adatok körének a hozzájuk tartozó adatkezelési céllal történő összepárosítása is, vagyis meg kell határozni, hogy az adott célra mely adatokat kezeli az applikáció. A felhasználó ugyanis akkor tudja felmérni azt, hogy az adatkezelés milyen hatással jár a magánszférájára, ha a kezelt adatok körét látja – ennek alapján tudja megítélni azt, hogy az adatkezeléshez hozzájáruljon-e vagy sem.

KEZELHETŐK-E AZ ADATOK MÁSODLAGOS CÉLOKRA?

Az egészségügyi szektor az, ahol a big data alkalmazása az egyének mindennapi életére különösen nagy hatással lehet. A big data által kinyerhető jobb adatok az mHealth alkalmazásokkal együtt számos előnnyel járnak mind a felhasználók, mind az egészségügyi ellátórendszer számára. Valamennyi mHealth alkalmazás esetében kulcskérdés ezért, hogy vajon másodlagos célokra, így különösen big data analitika, statisztika, tudományos kutatás céljára kezelhetők-e az alkalmazáson keresztül gyűjtött adatok. A big data analitika céljára történő adatgyűjtésnek és adatkezelésnek ugyanúgy meg kell felelnie az adatkezelési előírásoknak, mint bármilyen más célra történő adatgyűjtésnek és adatkezelésnek, vagyis a big data analitika sem jelent kivételt a jogszabályok alól. Ebből eredően a big data analitika sem lehet kifogás az adatok felhalmozására, raktározására, az üzleti vagy egyéb cél által indokoltnál hosszabb megtartására. A big data analitika alapvető elvei, törekvései és az adatkezelés európai uniós és magyar elvei között azonban alapvető ellentét feszül: míg a big data analitika célja az, hogy a megszerezhető összes adatot összegyűjtsék és kezeljék, historikus adatokkal együtt a lehető leghosszabb időre megőrizzék, tárolják, addig a jogszabályi elvek a fent már részletesen említett adatminimalizálás elvén nyugszanak, vagyis csak a minimálisan szükséges mennyiségű és fajtájú adat kerüljön kezelésre, és az is csak a cél eléréséhez feltétlenül szükséges ideig.

A fenti ellentétes érdekek feloldására több lehetőség is kínálkozik. A legegyszerűbb az, ha a big data analitikai, statisztikai, kutatási célt is feltüntetik az adatkezelési célok között, és ahhoz a felhasználó hozzájárul. Ha ez elmarad, és az alkalmazás üzemeltetője utólag kívánja ilyen új célra felhasználni az adatokat, kénytelen külön hozzájárulást kérni a felhasználóktól erre a célra, ami felhasználói élmény és marketing szempontjából nem előnyös, és nem is hatékony. Nem szükséges azonban azonnal elvetni a big data analitikai célú adatkezelést a felhasználói hozzájárulás beszerzésének nehézségei miatt: az adatok teljes anonimizálásával, maszkolásával, pszeudonimizálásával elkerülhető a hozzájárulás-kérés.

Mind az európai uniós, mind pedig a magyar jogszabályok alapján ugyanis a személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható; az érintettel pedig akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.[14]

A fenti előírás alapján tehát ha az adat már nem hozható kapcsolatba a felhasználóval, vagyis egy meghatározott személlyel, nem lehetséges egy meghatározott személyt azonosítani sem magából az adatból, sem adatok kombinációjából, és az adat kezelője nem tudja azonosíthatóvá visszaalakítani az anonim adatot, továbbá az anonimizált és eredeti adatok nem kapcsolhatók össze (pl. szervezeten belül), akkor az nem minősül személyes adatnak sem, így kezeléséhez nem szükséges hozzájárulás.

A teljes anonimizálás azonban a big data esetében általában nem lehetséges, ezért más technikák is szóhoz jutnak. Ilyen pl. az adatmaszkolás, ahol a neveket és a nyilvánvaló személyes azonosítókat törlik az adatokból, vagy a pszeudonimizálás (kódolás).

Ezek a technikák azonban nem teljes mértékben elégítik ki a fenti anonimizálási követelményeket, ezért alkalmazásuk esetén a big data célú felhasználáshoz való hozzájárulás még mindig kérdésként vetődik fel.

Az anonimizáláson kívüli megoldást jelenthet az, ha a big data analitikai célú adatkezelés összeegyeztethető a felhasználók által jóváhagyott eredeti adatkezelési célokkal. Általánosságban nem lehet olyan kijelentést tenni, hogy valamely adatkezelési cél összeegyeztethető, más pedig nem a big data analitikai céllal, ezt minden mHealth üzemeltetőnek esetről esetre kell megvizsgálnia.

Alapvetésként kijelenthető, hogy a big datától eltérő eredeti adatkezelési cél nem feltétlenül jelenti, hogy összeegyeztethetetlen a big datával. Ha a big data analitika célja trendek és összefüggések előrejelzése, akkor általában megengedett másodlagos adatkezelési célt jelent; míg ha a big data analitika célja egyének döntésének befolyásolása, akkor általában új célnak minősül, és a felhasználók külön hozzájárulása szükséges hozzá.[15]

KÖNNYEBB LESZ-E AZ MHEALTH APPOKNAK EZUTÁN?

Jövőre, 2018. május 25-én lép hatályba az Európai Parlament és a Tanács (EU) 2016/679. rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet – GDPR). A rendelet valamennyi uniós tagállam nemzeti adatvédelmi jogszabályának helyébe lép, így az Európai Unió teljes területén azonos szabályok lesznek érvényesek az adatkezelésre. Az országhatárokon átnyúló szolgáltatásokat nyújtóknak, így pl. az mHealth applikációk üzemeltetőinek előnyös lesz e változás, hiszen jövő évtől már csak egy rendeletnek való megfelelést kell biztosítaniuk az EU teljes területén, ami jelentős költségmegtakarítással jár.

A GDPR az amúgy is szigorú magyar szabályozáshoz és joggyakorlathoz képest szigorítást nem sok tekintetben hoz, a legtöbb rendelkezése eddig is létezett a magyar adatvédelmi jogban valamilyen formában.

Az mHealth applikációk szempontjából fontos újítása lesz az EU-s rendeletnek, hogy a hatályos magyar jogszabályokkal ellentétben nem kér írásbeli hozzájárulást az egészségügyi adatok kezeléséhez, viszont a többi személyes adathoz képest szigorúbb, „kifejezett" hozzájárulást kíván meg. Ez a gyakorlatban azt fogja jelenteni, hogy a felhasználónak az egészségügyi adatai kezeléséhez elkülönülten, kifejezetten hozzá kell járulnia, a hozzájárulás formája azonban megegyezik a többi személyes adatéval: egyértelmű és határozott hozzájárulásnak kell lennie, amely a mostani magyar szabályozással szemben megtehető elektronikusan is, pl. checkbox kipipálásával. A GDPR azonban hagy egy kiskaput a nemzeti kormányoknak, amelyeknek lehetőségük lesz többek között éppen az egészségügyi adatokra saját szabályozást kialakítani, így a magyar kormányzat elvben fenntarthatja az egészségügyi adatok kezelésére vonatkozó, a rendeletnél szigorúbb írásbeli hozzájárulás követelményét. A GDPR hatályba lépése előtt egy évvel nincs még konkrét magyar jogszabály, amely ezt kimondaná, de a magyar adatvédelmi hatóság nyilatkozatai és a szigorúbb magyar szabályozás egyes elemeinek fenntartására vonatkozó tervei alapján nem zárható ki ennek lehetősége. Egy ilyen szabályozás a magyar mHealth applikáció fejlesztőket az egységes uniós piacon versenyhátrányba hozhatja; akadályozhatja, hogy az EU többi tagállamában elérhető mHealth szolgáltatások azonos feltételekkel és módon legyenek itthon is elérhetők.

Az EU rendeletétől eltérő nemzeti szabályozás lehetősége önmagában is megnehezíti a vállalkozásoknak a GDPR-re való, amúgy is jelentős erőforrásokat igénylő felkészülést, különösen ha az ilyen nemzeti szabályozás esetlegesen a felkészülési időszak második felében, a felkészülés finisében születik meg, nem hagyva elegendő időt az adaptálására és az addigi felkészülés esetleges módosítására.

Levelezési cím:
katalin.horvath@sarandpartners.hu

Irodalom:

1. Kotz D, Gunter CA, Kumar S, Weiner JP. Privacy and Security in Mobile Health: A Research Agenda. IEEE Computer Society, 2016. www.computer.org/computer
2. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) 3. § 2. pontja
3. 1997. évi XLVII. törvény az egészségügyi adatok kezeléséről és védelméről 3. § a) pontja
4. Code of Conduct on privacy for mobile health application. Európai Bizottság, 2016. https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised
5. Infotv. 20. § (2) bekezdése alapján
6. Infotv. 4. § (2) bekezdése alapján
7. Magyarország Alaptörvénye VI. cikk (2) bekezdése
8. Infotv. 20. § (2) bekezdése
9. Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről, 2015. szeptember 29. https://www.naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf
10. Az előzetes tájékoztatás követelményéről további részletek az Európai Bizottság Adatvédelmi Munkacsoportja által kibocsátott, 15/2011. számú véleményben. Az Adatvédelmi Munkacsoport az adatvédelemmel, valamint a magánélet védelmével kapcsolatos kérdésekkel foglalkozó, független európai tanácsadó szerv. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_hu.pdf
11. Infotv. 3. § 7. pontja: //hozzájárulás:// az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez
12. Infotv. 5. § (2) bekezdés a) pontja
13. Infotv. 4. § (1) és (2) bekezdés és 20. § (2) bekezdés
14. Infotv. 4. § (3) bekezdése
15. A big data adatvédelmi összefüggéseiről és kérdéseiről és az új adatvédelmi rendelet összefüggéseiről további részletek itt: Big Data, artificial intelligence, machine learning and data protection. Information Commissioner's Office (ICO), Egyesült Királyság, 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

A cikkhez csatlakozóan további felhasznált és ajánlott irodalom található az otszonline.hu weboldalon.