2018. szeptember 29. a nap, amelytől kezdődően az eIDAS rendelet alapján minden közigazgatási szolgáltatás, amely felhasználók beazonosítását írja elő, köteles elfogadni akár a más országok által szolgáltatott adatokat is, ha az azonosítás erősségének szintje megfelelő. Ez a határokon átívelő kommunikáció alapvető fontosságú az Egységes Digitális Piac (Digital Single Market, DSM) továbbfejlődése szempontjából.

Ezen alkalomból jelent meg a MELASZ (Magyar Elektronikus Aláírás Szövetség) és a FinTechZone által egy közösen írt cikk a hírportálon.

Újabb adatvagyon nyílik. Erre a "csodafegyverre" vártak a magyar bankok (is)

A közhiteles adatvagyon megnyitásával a webshopok kiszűrhetik a hamis rendeléseket, egyszerűbbé válik az online számlanyitás, könnyebbé válik a beiratkozás az oktatási intézményekbe és egyre kevesebb adatot kell megadnunk az elektronikus űrlapok kitöltéséhez. Az előírt közhiteles adatokon kívül a hazai piaci szereplők rövid időn belül automatizálhatják hozzáférésüket a céges és az egyéni vállalkozói adatokhoz is. Ez utóbbi a bankok számára "csodafegyver" lesz új online szolgáltatások elindításához.

A közhiteles adatbázisok megnyitása új dimenzióba emeli majd a távollévők között kötendő szerződések "bizalmi" szintjét, a csalások minimalizálása pedig kedvezményesebb árakat is eredményezhet pl. a webshopoknál. Egyelőre akadnak még adminisztratív és műszaki, üzemeltetési akadályok, de jogilag a közhiteles adatbázisokhoz való automatizált hozzáférésre már 2018. január 1-től lehetősége lenne a piaci szereplőknek is.

A szabályozás háttere

Az eIDAS (910/2014/EU Rendelet az Elektronikus Azonosítási és Bizalmi Szolgáltatásokról) kimondja, hogy meg kell nyitni a közigazgatás közhiteles adatbázisait a közigazgatási szakrendszerek és a piaci szereplők előtt – határon átnyúló ("cross-border") módon, az Európai Unión belül.

Az EU által kötelezően előírt 8+10+2 adat (attribútum) listája itt érhető el. Ezen felül Magyarországon ennél több közhiteles adat is érhetővé válik. A magyar nevezéktanban pl. TAJ és NAV okmányazonosító, illetve hamarosan a céges és egyéni vállalkozói teljes adatlap is elérhető lesz. (Ha belegondolunk, akkor ez a 8+10+2 lekérhető közhiteles adat sok folyamathoz elegendő lesz, pl. egy egyszerű, webshopos rendeléshez (viselt név, lakcím kell hozzá), vagy szerződés megkötéséhez is.)

Piaci szereplők hozzáférése a közhiteles adatbázisokhoz

A közhiteles adatbázisokhoz a közigazgatási szakrendszerek, illetve más, nem piaci szereplők már 2017. január 1. óta hozzáférhetnek (pl. Diákhitel Központ, lásd: " Egyedülálló újítás: hallgatói hiteligénylés személyes megjelenés nélkül
").

A 451/2016. (XII. 19.) Korm. rendelet 68/A. § alapján a piaci szereplők a díjtáblázat szerinti díjak megfizetése ellenében hozzáférhetnek a közhiteles adatbázisokhoz. A műszaki specifikációk is adottak 2008 óta, mivel már egy bevált, az akadémiai szférában régóta használt protokollt írtak elő (OASIS SAML).

A piaci szereplőknek a hozzáféréshez egyrészt kérvényezniük kell a hálózathoz való csatlakozást az adott ország felelősénél (Magyarországon: NISZ, Nemzeti Infokommunikációs Szolgáltató Zrt.), másrészt rendelkezniük kell a felhasználó felhatalmazásával az adatai eléréséhez.

A közhiteles adatbázisok gyakorlati hasznosítása

Nem csak a PSD2 (Második Pénzforgalmi Irányelv) kapcsán megnyíló banki adatvagyonra, hanem a pontos, közhiteles adatok lekérdezésére alapozva is számos új szolgáltatást lehet majd kialakítani.

Az online bankszámlanyitáshoz, vagy a közmű szolgáltatókkal kötendő elektronikus szerződésekhez a természetes, vagy a jogi személy adatait már a közhiteles adatbázisból lehet majd feltölteni (a GDPR-nak, az Általános Adatvédelmi Rendeletnek megfelelően), így egyszerűbbé és gyorsabbá válhat az ügyintézés.

Az EU tervei szerint 2-3 éven belül az egészségügyi adatok is lekérdezhetők lesznek ugyanezen hálózaton keresztül, így az egészségbiztosítások esetén nem kell külön állapotfelmérésre elküldeni az új ügyfelet, hanem elég lesz lekérdezni a kórelőzmény adatait.

Összességében

A műszaki specifikációk és a jogi feltételek adottak. Ezen felül az is adott, hogy mi az a 8 természetes személyre és 10+2 jogi személyre vonatkozó adat, amit szolgáltatni kell.

Az adatok köre várhatóan bővülni fog, hiszen már most felmerült az állampolgárság, vagy az édesanyja születési neve attribútumok iránti igény. A piaci szereplők – többek között a bankok is – már nagyon várják a Belügyminisztérium által jóváhagyott csatlakozási engedélyeket, hogy elindulhassanak az új online szolgáltatások.

Mélyvíz: Összefüggések

Mi köze van az eIDAS rendeletnek a PSD2 irányelvhez?

1. mindkét területen megjelenik a felhasználók erős hitelesítése (Strong Customer Authentication, SCA) követelmény;

2. mindkét területen megjelenik az adathozzáférési jogosultságok felhasználó általi kezelése (Consent-based provisioning);

3. mindkét területen megjelenik az adatbázisok megnyitása szabványos felületeken keresztül és a felhasználói adatok elérhetősége harmadik felek – akár piaci szereplők – számára (Open Banking API és OASIS SAML);

4. mindkét területen megjelenik az adatok (pl. űrlapok, fizetési műveletek) hitelesítése.

(1) A felhasználók erős hitelesítése

Az erős felhasználó-hitelesítés a PSD2 irányelv esetén legalább kétfaktoros megoldás alkalmazását írja elő, ami védett a módosítás ellen és az adott tranzakcióhoz köthető. Ez megfelel az eIDAS végrehajtási rendeletében leírt közepes, azaz jelentős szintnek, ahol két, különböző megoldást kell alkalmazni. A jelszavak, kulcsok tárolására viszont ez a szint még engedi a szoftveres megoldásokat is, azaz akár egy mobilos, egyszeri jelszavas alkalmazás is elegendő lehet. (A magas biztonsági szinten azonban már mindenképpen hardveres megoldás szükséges, mint az eSzemélyi kártya.)

A kétfaktoros felhasználó-hitelesítés megjelenik több folyamatnál is, mint pl. banki szektor számára érdekes valós idejű ügyfél-átvilágítás kapcsán, ami akár az ügyfelekkel való rendszeres adategyeztetési követelményt is meg tudja oldani, ha a Proof-of-Presence (PoP) követelmény teljesül.

(2) Az adathozzáférési jogosultságok

Nem volt véletlen, hogy a GDPR rendelet 2018. május 25-én élesedett (a korábbi adatvédelmi irányelv hatályának elvesztésével), hiszen szükség volt egy jogilag erősebb (irányelv helyett rendeleti) szintű és komolyabb szankciókat is meghatározó szabályozásra, amely alapján az érintett, igazolható módon a hozzájárulását tudja adni személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Igaz, hogy végrehajtási rendeletek és műszaki specifikációk hiányában a legtöbb GDPR követelmény megmaradt keretszabály szintjén, de a hozzájárulást mind a PSD2 irányelv, mind az eIDAS rendelet komolyan veszi.

A közigazgatási szakrendszerek (public service provider) számára ingyenesen kell biztosítani a felhasználó hitelesítését és ennek kapcsán a beazonosításhoz szükséges adatok, attribútumok lekérdezését, azonban a piaci szereplők (private service provider) csak díj megfizetése, illetve a felhasználó által megadott hozzájárulás ellenében vehetik igénybe ugyanezen szolgáltatást.

(3) Az adatbázisok megnyitása

Az erős felhasználó-hitelesítés után a felhasználó engedélyezheti a szolgáltatás számára, hogy több más adatát, attribútumát is lekérdezze a Know-Your-Customer (KYC) követelménynek való megfelelés érdekében.

A banki adatbázisok is értékes adatokat tartalmaznak a felhasználókról magukról, illetve azok

vásárlási szokásairól, fizetési hajlandóságáról, hitelképességéről (Account and Transaction API), de a közigazgatásban elérhetővé válnak olyan adatforrások (pl. a Személyiadat- és Lakcímnyilvántartás vagy az eSzemélyi okmányon tárolt adatok), amelyek közhitelesnek, azaz jogilag megbízhatóbbnak számítanak.

Minden EU tagállamnak tudnia kell szolgáltatni néhány természetes személyre, illetve jogi személyre (pl. cégekre) és azok képviselőire vonatkozó közhiteles attribútumot határokon átívelően, aminek révén könnyebbé válhat az egyes szolgáltatások kinyitása más országok felé (pl. online onboarding folyamat: máltai banknál számlanyitás magyar állampolgár számára vagy valós idejű ügyfél-átvilágítás, adategyeztetés videochat rendszeren keresztül születési adatok, viselt név, lakcím, állampolgárság lekérdezése révén).

(4) Az adatok hitelesítése

Maga az eIDAS rendelet a korábbi e-aláírási irányelv jogutódja, azaz a dokumentumok, űrlapok hitelesítése továbbra is a szabályozás középpontjában áll.

A PSD2 irányelv az e-aláírásról közvetlenül nem ír, de külön cikkben jelenik meg a fizetési műveletek hitelesítésének és teljesítésének bizonyítása, ami akár blokkláncba (blockchain) szervezve is megvalósítható. Ehhez kézenfekvő lehet az e-aláírási technológia alkalmazása, akár az eSzemélyi kártya révén, ami nem csak a hazai, de tagállamok közötti hiteles dokumentumközlekedtetéshez is megfelelő jogilag.

Honnan indult és hová tart az eIDAS rendelet mögötti háttérrendszer?

Az eIDAS rendelet kapcsán a közigazgatási szektorban (GovTech) most elinduló rendszereket korábban Shibboleth név alatt az akadémiai szektorban (EduTech) már sikerrel bevezették – eduID azonosítóval tudnak bejelentkezni és akár más intézmények tanulmányaihoz hozzáférni -, de a következő néhány évben csatlakozni fog az egészségügyi szektor (HealthTech) is a CBH irányelv miatt. Ezek mellett jelenik meg – hasonló célkitűzésekkel, de kicsit más műszaki megoldással – a banki szektor (FinTech) a PSD2 irányelv révén.

Mindegyik szektornál egységes felhasználó-hitelesítési, beléptetési lehetőségek lesznek elérhetők, illetve egységes adathozzáférési jogosultságkezelés. A közös, határokon átívelő kommunikációs hálózaton egyre többféle adat válik elérhetővé, amelyek többféle folyamatot, szolgáltatást tudnak majd megtámogatni.

Aki – akár piaci szereplőként – csatlakozik ezekhez a rendszerekhez, az nem csak a fizetési folyamatokat tudja megújítani, de a megrendelési, számlázási, szállítási lépésekhez is hozzá tudja tenni a közhiteles adatforrásokból származó adatokat, az egészségügyi szolgáltatásokat pedig akár a kórelőzmény adatok lekérdezésével, elemzésével tudja még tovább okosítani.

FinTech	EduTech	GovTech	Hea
Directive 2015/2366/EU (PSD2)	-	Regulation 910/2014/EU (eIDAS)	Directive 20
Regulation 2016/679/EU (GDPR)	Regulation 2016/679/EU (GDPR)	Regulation 2016/679/EU (GDPR)	Regulation 201
2018-01-13 → 2019-03-13	-	2018-09-29	
strong customer authentication 2FA with SW/HW: TOTP, SSL/TLS, eID	simple customer authentication 1FA with SW: UID/PWD (eduID)	strong customer authentication 2FA with SW/HW: TOTP, SSL/TLS, eID	strong custom 2FA with SW/HW:
consent-based provisioning access control rules + attribute queries e.g. Consent Manager	consent-based provisioning access control rules + attribute queries e.g. Higher Education eXternal Attribute Authority (HEXAA)	consent-based provisioning access control rules + attribute queries e.g. Rendelkezési Nyilvántartás (RNY)	consent-bas access control rule e.g. Digitális Ön
e.g. databases of banks	e.g. databases of universities	e.g. databases of governments	e.g. databas
attributes of Account and Transaction Payment Initiation	attributes of user properties: 22 institutional relationship: 3 educational use: 7	attributes of natural person (representative): 8 + 2 legal person: 10	attri HealthCare Profe Patient Identity +
OpenID Connect / Open Banking API	OASIS SAML / eduID specifications	OASIS SAML / eIDAS specifications	OASIS SAML / e