ADATVÉDELMI ÉRTELMEZŐ SZÓTÁR

- ***adatvédelem: a*** személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

- ***személyes adat:*** bármely meghatározott, azonosított vagy azonosítható természetes személlyel [érintett] kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

- ***adatalany/érintett:*** bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

- ***különleges adat:*** a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat.

- ***bűnügyi személyes adat:*** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

- ***adatkezelés:*** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése.

- ***adatkezelő:*** az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

- ***adatfeldolgozás:*** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).

- ***adatfeldolgozó:*** az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.

- ***érintett jogai:*** az adatalanyt még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor egyértelműen tájékoztatni kell az adatkezelés minden részletéről. Az érintett kérheti adatai helyesbítését, bizonyos esetben törlését is, valamint törvényben meghatározott esetekben tiltakozhat személyes adatai kezelése ellen.

- ***az adatkezelés jogalapja***: főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.

- ***hozzájárulás:*** az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Különleges adatok esetében szükséges az írásos forma.

- ***megfelelő tájékoztatás:*** az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

- ***tiltakozás:*** az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

- ***adatbiztonság:*** az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.

- ***az adatkezelés elvei:*** a célhoz kötött adatkezelés követelménye (lásd alább), valamint az adatminőség követelménye. Ez utóbbi magában foglalja a pontos, teljes és naprakész adatok igényét, valamint az adatfelvétel és az adatkezelés tisztességes, törvényes mivoltát.

- ***célhoz kötött adatkezelés:*** személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és - ha az adatkezelés céljára tekintettel szükséges - naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

- ***adattovábbítás külföldre:*** személyes adatok továbbítása EGT-n (Európai Gazdasági Térség: az Európai Unió országai, valamint Izland, Norvégia és Liechtenstein) kívüli, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz.

- ***információszabadság:*** a közérdekű, valamint közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, mely elősegíti a közhatalom gyakorlásának demokratikus kontrollját és a közintézmények átláthatóságát (transzparencia).

- ***közérdekű adat:*** az állami/önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől (így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat).

- ***közérdekből nyilvános adat:*** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. (pl. a hitelezői érdekek védelme, valamint a piaci forgalom biztonsága érdekében az adatok széles körét minősíti közérdekből nyilvánosnak az ingatlan-nyilvántartásról szóló törvény, a cégtörvény, valamint a számviteli törvény)

- ***Avtv.:*** 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, a rendszerváltás utáni első adatvédelmi törvény, mely 2011. december 31-ig volt hatályban. 2012. január 1-től hatályon kívül helyezte az Infotv. (lásd alább).

- ***Infotv.:*** 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, amelyet az Alaptörvény VI. cikke alapján az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, az ezen jogok érvényesülését szolgáló alapvető szabályokról, valamint az ellenőrző hatóságról (NAIH) alkotott. A törvény célja, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon. 2012. január 1-től hatályos.

- ***NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság:*** az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.

- ***EDPS (European Data Protection Supervisor):*** a 2004-ben létrejött európai adatvédelmi biztos független intézményként felügyeli az európai intézményekben és uniós szervekben folyó személyes adatok kezelését, emellett az európai adatvédelmi joggyakorlat és jogértelmezés kialakításában is kulcsszerepe van.

- ***belső adatvédelmi felelős:*** az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős.

- ***Európa Tanács Adatvédelmi Egyezménye:*** az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény (az Európa Tanács ún. 108-as Egyezménye). Az első jelentős, az aláíró államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Magyarországon kihirdette az 1998. évi VI. törvény, 1998. február 27-én.

- ***uniós adatvédelmi irányelv:*** az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az Európai Unió 1995. október 24-én született általános adatvédelmi irányelve, mely – többek között – létrehozta az ún. 29-es Adatvédelmi Munkacsoportot (lásd alább).

- ***29-es Munkacsoport:*** A 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosaiból, illetve adatvédelmi hatóságainak képviselőiből álló független tanácsadó, véleményező és konzultatív fórum. Állásfoglalásaival és javaslataival segíti az Európai Bizottság munkáját az európai polgárok információs önrendelkezési jogának védelme érdekében.

- ***uniós adatvédelmi szabályozás-tervezet (Data Protection Regulation – the „Proposed Regulation"):*** a jogi csomagként 2012-re előkészített anyag egyrészt magában foglalja az általános uniós adatvédelmi rendelet tervezetét (lásd alább), valamint a rendőrségi és bűnügyi igazságügyi adatkezeléseket szabályozó irányelv tervezetét.

- ***uniós adatvédelmi rendelet-tervezet:*** az Európai Bizottság 2012. január 25-én közzétett javaslata, melynek célja az európai adatvédelmi szabályok átfogó reformja és ennek keretében egy uniós szinten egységesebb, egyszerűbb és korszerűbb szabályozás kialakítása az európai polgárok adatainak kezelése érdekében. A rendelet, mint jogforrás (az irányelvtől eltérő módon) közvetlenül hatályosul az uniós tagállamokban, ami a tényleges, azonnali és feltétlen jogharmonizációt garantálja uniós szinten. A tervezetet először a tagállamok és az Európai Parlament is megvitatja, majd ha az Európai Parlament elfogadja, két év szükséges a hatályba lépéshez.

- ***Schengen/SIS:*** a schengeni térség létrehozása a személyek szabad mozgását lehetővé tevő legfontosabb uniós vívmány. A belső határok eltörléséből és a külső határok megszigorított ellenőrzéséből eredő biztonsági kockázatokat a Schengeni Információs Rendszer (SIS), Európa legnagyobb informatikai rendszere hivatott kezelni, elsősorban a hatékony adatmegosztás eszközével. A tagállamok keresett és eltűnt személyekkel, ellopott vagy elveszett tulajdonnal, beutazási tilalmakkal kapcsolatos adatokat – úgynevezett figyelmeztető jelzéseket – helyeznek el a SIS-ben. Az érintettek SIS-sel kapcsolatos adatvédelmi kéréseikkel (például tájékoztatási vagy helyesbítési kérelem) bármely rendőrkapitánysághoz vagy magyar külképviselethez fordulhatnak, akik ezt továbbítják az ORFK NEBEK SIRENE Irodához. A magyar SIS adatkezelések jogszerűségét a NAIH felügyeli.

- ***EURODAC: (European Dactyloscopy);*** a 2725/2000/EK rendelet által életre hívott európai ujjnyomat nyilvántartó adatbázis, melynek elsődleges célja a menedékkérők és illegális migránsok beazonosítása.

- ***OECD irányelvek:*** a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvei, melyek 1980. szeptember 23-án léptek életbe.

- ***BCR (Binding Corporate Rules – Kötelező Erejű Vállalati Szabályok):*** multinacionális társaságok által alkalmazott és a bejegyzés székhelye szerinti EU-tagállam adatvédelmi hatósága által jóváhagyott kötelező magatartási kódex. Ennek értelmében a multinacionális cégcsoport vállalja, hogy a vállalatcsoporton belüli, az EU tagállamok területéről harmadik, nem uniós országba történő adattovábbítás során megfelelő, a célországban egyébként szokásosnál nagyobb szintű védettséget biztosít az általa továbbított személyes adatoknak.

- ***ACTA (Anti-Counterfeiting Trade Agreement – Hamisítás elleni kereskedelmi megállapodás):*** nemzetközi megállapodás, melynek deklarált célja az interneten terjedő kalóztartalmakkal szembeni hatósági fellépés lehetőségének megteremtése. A megállapodás hivatalos előterjesztője Japán volt, a dokumentum 2011 márciusában nyílt meg aláírásra. A megállapodás létrehozására irányuló nemzetközi tárgyalások folyamán az európai adatvédelmi biztos (EDPS) 2010 februárjában kiadott véleményében a dokumentum uniós adatvédelmi szabályokkal való összeegyeztethetőségével kapcsolatban aggályát fejezte ki - az Európai Unió nem csatlakozott hozzá.

- **BAR-lista**: a magyar Központi Hitelinformációs Rendszer (KHR) korábbi elnevezése. A KHR a lakossági banki ügyfelek vonatkozásában két alrendszerből áll. A negatív listás alrendszerben található a késedelmes adósok hitelmulasztással kapcsolatos adatai, míg a pozitív listás rendszer tartalmazza valamennyi magyarországi hitelfelvevő, hitelintézetek által átadott ügyfél- és szerződésadatait. Ez utóbbi alrendszerből a bankok hiteltörténeti adatokat csak abban az esetben hívhatnak le, ha a hozzájuk forduló hiteligénylő a hitelképességének pontosabb megítélése érdekében ehhez kifejezetten hozzájárul.

- ***CCTV (Closed-Circuit Television): zárt láncú televíziós megfigyelési rendszer,*** mely több kamerából áll, és amelynek célja egy adott terület biztonsági célú állandó megfigyelése. Ellentétben a nyilvánosan közvetített, „nyílt láncú" televíziós adásokkal, a CCTV felvételei csak egy zárt csoport számára (általában a biztonsági személyzetek számára) nyilvánosak. A CCTV-rendszerek széleskörű elterjedése vitákat váltott ki a személyhez fűződő jogokat és adatvédelmet érintő esetleges negatív következmények miatt.

- ***PNR* (*Passenger Name Records):*** a légiutas-nyilvántartási adatállomány elsősorban az utas által a foglalás során megadott és a légitársaság által az utazással összefüggésben összegyűjtött adatokból áll, melyeket a légitársaságok és a repülőtéri irányító központok tárolnak, azonban ezekhez bűnüldöző hatóságok is bizonyos esetekben hozzáférést kapnak, kaphatnak. Az adatok kezelésének uniós szabályozása jelenleg is folyamatban van, az egyes adatvédelmi kérdések különös megfontolásokat igényelnek. A korábban sok vitát kiváltó, a légi utasok adatcseréjéről szóló, az EU és az Egyesült Államok közötti egyezmény 2012. július 1-én lépett hatályba.

- ***cloud computing:*** („számítástechnikai felhő", „felhő alapú informatika"): a számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások

közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (pl.: Gmail), vagy az online tárhelyek (pl.: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.

- ***cookie-k („sütik"):*** rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat [kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek] csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetőek a felhasználó böngészési szokásai.

- ***privacy by default:*** olyan adatvédelmi irányzat, melynek lényege, hogy személyes adatok gyűjtésére, kezelésére, illetve feldolgozására csak és kizárólag az adatalany kifejezett kérésére kerülhet sor. Az adatkezelők alapvető, „alapértelmezett" (angolul: by default) hozzáállása az kell, hogy legyen, hogy minden körülmények között figyelembe veszik az adatvédelmi szempontokat és ezeknek megfelelően járnak el az adatkezelési műveletek során.

- ***privacy by design:*** Kanadában, az 1990-es években kialakult adatvédelmi irányzat. Lényege, hogy az adatvédelmi szempontoknak megfelelő gyakorlat nem merülhet ki a hatályos szabályozásnak való formális megfelelésben. Az adott szervezet alapvető működési elve az adatvédelmi szempontoknak való megfelelés, ezért működését, struktúráját ezek maximális figyelembevételével alakítja ki, az adatvédelmi szempontokat már az egyes működési fázisok megtervezésekor beépíti és így biztosítja az adatvédelem teljes körű érvényesülését. Rokon területe a „privacy by default" megközelítésnek.