

## **Adatvédelmi kiadvány**

1. **Adatvédelem:** a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.
2. **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.
3. **Adattulajdonosi és önrendelkezési jog:** alaptörvényben rögzített jog, az ezzel összefüggő jog csak képviselői jelenléti 2/3-os törvénnyel (sarkalatos törvény) módosítható.
4. **Egészségügyi adat:** testi és/vagy lelki állapotunkra vonatkozó adatok, melyeket gyógyító-megelőző betegellátás során állapítanak meg. Különleges, fokozott védelmet igénylő adatok. A mindennapi gyakorlatban a személyes adat + egészségügyi adat együttesen értelmezhető és kezelhető, ill. feldolgozható, a személyazonosító adatoktól értelemszerűen nem szakítható el.
5. **Ismeret:** valamilyen adatobjektummal kapcsolatos tapasztalataink, általánosításaink és fogalmaink összessége, az információ egyik lehetséges forrása.
6. **Információ:** olyan adat, vagy ismeret, amely a viselkedésünket befolyásolni képes.
7. **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.
8. **Különleges adat:** a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre, az egészségi állapotra, valamint a kóros szenvedélyre vonatkozó és a bűnügyi személyes adat. Adattulajdonos rendelkezik a hozzáféréssel, fokozott védelmet igénylő adat.
9. **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.
10. **Adatkezelés:** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet. Ilyen 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.

11. **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.
12. **Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).
13. **Adatfeldolgozó:** az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.
14. **Közös adatkezelés:** a természetes személy személyes adatának meghatározott jog, vagy jogosultsághoz tartozó érvényesítése legalább két, vagy több adatkezelő, ill. adatfeldolgozó együttes tevékenységét igényli.
15. **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.
16. **Az adatkezelés jogalapja:** főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.
17. **A jogszerűség elve:** a rendelet kimondja, hogy személyes adatok csak jogszerűen kezelhetők. A jogszerűség azt jelenti, hogy az adatkezelő csak a rendelet által meghatározott esetekben és jogalapokon kezelheti az adatokat. Így például akkor, ha ahhoz a magánszemély hozzájárult, vagy hozzájárulás nélkül akkor is, ha az adatkezelés valamilyen jogi kötelezettség teljesítéséhez szükséges (például adóbevallás benyújtása, munkavállaló NAV bejelentése). Nem kell hozzájárulást kérni akkor sem, ha az adatkezelés ahhoz szükséges, hogy az adatgazdával kötött szerződést teljesíteni tudja a vállalkozó (például bankszámla adatok a megbízási díj átutalásához). Ugyanígy jogszerű az adatkezelés akkor, ha az adatkezelés az adatkezelő vagy valaki más jogos érdekének érvényesítéséhez szükséges.
18. **Az átláthatóság elve:** az átláthatóság elve arra kötelezi az adatkezelőket, hogy a rendeletnek megfelelően, könnyen érthető és hozzáférhető formában, világosan, írásban vagy elektronikusan tájékoztassák a magánszemélyeket arról, hogy milyen adataikat, milyen célra, milyen jogalapon, hogyan kezelik. Ennek praktikusán az adatkezelési

szabályzatban lehet eleget tenni. Az átláthatóság másik követelménye az, hogy ha a magánszemély tájékoztatást kér adatai kezeléséről (hozzáférési jog gyakorlása), akkor azt az adatkezelő a jogszabálynak megfelelő határidőben, módon és tartalommal teljesíti.

19. **Az elszámoltathatóság elve:** az adatvédelem új „szuperalapelve”, egy elv mindenekfelett. Lényegében azt jelenti, hogy az adatkezelőnek teljes egészében meg kell felelnie a rendelet követelményeinek, ennek érdekében különböző intézkedéseket kell tennie és ezt bizonyítania is tudni kell. Ide tartozik például az adatbiztonság betartása, a személyzet adatvédelmi oktatása, adatvédelmi nyilvántartás vezetése, érintetti jogok gyakorlásával kapcsolatos belső eljárások kialakítása, információbiztonsági szabályzat elkészítése, adatkezelési folyamatok ellenőrzése, adatvédelem beépítése az üzleti folyamatok tervezésébe, adatbiztonsági incidensek kezelésére folyamatok kialakítása. Ezeket továbbá az adatkezelőnek mind dokumentálnia kell és meg kell őriznie a megfelelés igazolására.
20. **A célhoz kötöttség elve:** személyes adatokat gyűjteni, felhasználni, kezelni csak meghatározott, egyértelmű és jogszerű célból lehet. Az adatkezelési célokat az adatkezelési tájékoztatóban adatkategóriánként kell megjelölni, és az egyes adatok csak a hozzájuk rendelt célokból kezelhetők, más célra nem használhatók fel. Így például, ha az e-mail címet azért kérik el, hogy regisztráljanak egy webshopban, akkor a webshop nem lesz jogosult erre az e-mailcímre később hírlevelet, ajánlatokat küldeni, vagy azt másoknak eladni, mert az eredeti és közölt adatkezelési cél a webshopban történő regisztráció és vásárlás volt.
21. **A pontosság elve:** az adatkezelésben nagyon fontos, hogy mindig olyan adatokat kezeljenek, amelyek naprakészek, pontosak. Így például, ha valakinek megváltozott a neve vagy az e-mail címe, és ezt bejelenti ahol regisztrált, akkor az, köteles lesz azt az adatbázisában javítani és a régi adatot törölni.
22. **Az adattakarékosság elve:** röviden azt jelenti, hogy nem lehet „készletre” adatot gyűjteni, vagyis csak olyan adat kérhető be, amely az adatkezelési cél szempontjából feltétlenül szükséges, megfelelő és releváns – azaz a lehető legkevesebb adatot kell kezelni. A gyakorlati adattakarékosságnak ugyanakkor ésszerű és a relevanciát nem érintő adatminimalizálás követelményeinek feltétlenül eleget kell tennie, azaz az adattakarékosság nem lehet olyan mértékű és tartalmú, amely a személyazonosítást akadályozza, vagy kétségessé teszi, másrészt akadályt jelent a természetes személy valamely jogának, ill. jogosultságának az érvényesítésében.
23. **A beépített és alapértelmezett adatvédelem elve:** az adatkezelők kötelesek megfelelő intézkedésekkel biztosítani a rendelet szerinti jogszerű adatkezelést, és gondoskodni az általuk kezelt személyes adatok biztonságáról. Az alkalmazott intézkedéseknek, módszereknek mindig az adott cég által végzett adatkezelés és a kezelt adatok jellegéhez, a fennálló lehetséges adatkezelési kockázatokhoz kell igazodnia, vagyis például egy egészségügyi adatokat kezelő orvosi rendelőnek, vagy banki adatokat kezelő banknak sokkal magasabb szintű védelmet, komolyabb titkosítást, álnevesítést, jogosultságkezelést

és egyéb intézkedéseket kell alkalmaznia, mint például egy cipőwebshop üzemeltetőjének. Az adatkezelés, adatvédelem elveit pedig már a szoftverfejlesztéskor, az üzleti folyamatok tervezésekor figyelembe kell venni, nem csupán a végén.

24. **Az elfeledtetéshez való jog:** minden magánszemélynek joga van ahhoz, hogy ha kéri, vagy ha az adatkezelési cél már megvalósult, akkor adatait az adatkezelő törölje. Ennek a törlésnek mindent érintenie kell, vagyis a magánszemélyt mindenhol „ki kell radírozni”, mintha soha nem lettek volna adatai az adott cégnél, azaz az érintett kérheti az adatkezelőt, hogy „felejtse el”. Az adatkezelő nem minden esetben köteles azonban a magánszemély adatait törölni, így például megtagadható a törlési kérelem, ha az adat jogi kötelezettség teljesítéséhez szükséges (például számla kiállításához, adóbevallás benyújtásához, stb.), vagy ha a jogszabály szerint az adatkezelő az adatokat őrizni köteles (például számviteli, TB és adójogi előírások).
25. **Adathordozhatóság:** a magánszemélyek olyan szolgáltatóknál, ahol adataikat automatikusan kezelik (például számítógéppel), kérhetik, hogy a szolgáltató adja át ezeket az adatokat egy másik szolgáltatónak. Ilyen eset fordul elő például mobiltelefon, internet, tv előfizetés váltás esetén, számhordozásnál. Fontos, hogy papíron kezelt, anonimizált, titkosított adatokra nem kérhető, és csak a hozzájárulás alapján kezelt adatokat adják át a szolgáltatók ez alapján.
26. **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.
27. **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.
28. **Tiltakozás:** az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
29. **Adatbiztonság:** az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.
30. **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.

31. **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.
32. **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.
33. **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).
34. **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). Nem titkolható adat.
35. **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).
36. **GDPR:** az Európai Parlament és a Tanács 2016. április 27.-ei (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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).
37. **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 tartásuk, valamint a közügyek átláthatósága a közérdekű és a

közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon. 2012. január 1-től hatályos. Az Infotv. 2018. július 01.-től, majd 2018. június 25.-től GDPR szerinti jogharmonizációs módosításra került.

38. **NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság:** az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos korábbi intézményét felváltó nemzeti adatvédelmi hivatal, melynek feladata a két információs jog (biztonság és önrendelkezés) védelme és a magyarországi adatkezelések és adatfeldolgozások törvényességének felügyelete. A korábbi NEIH 2018. július 01.-től kezdődően már információs hatóság, a NAIH, melynek feladata, hatásköre és felelősségi viszonyai, szankcionálásai az Infotv.-ben rendezettek.
39. **EDPS (European Data Protection Supervisor):** a 2004-ben létrejött európai adatvédelmi biztos független intézményként felügyeli az európai intézményekben és uniós szervezetekben folyó személyes adatok kezelését, emellett az európai adatvédelmi joggyakorlat és jogértelmezés kialakításában is kulcsszerepe van.
40. **Adatvédelmi tisztviselő:** az őt megbízó szervezeten belül tanácsokat ad és ellenőriz, ezzel biztosítva azt, hogy mind egyéni, mind szervezeti egység, mind pedig az egész szervezet szintjén a GDPR rendelkezéseinek megfelelően történjen az adatkezelés és az adatfeldolgozás.
41. **Adatsértés:** GDPR rendelkezéseit tudatosan, vagy gondatlanul megsértő adatkezelés, adatfeldolgozás. Adatvédelmi tisztviselő által hivatalból, vagy bejelentés alapján minden esetben kivizsgálendő, minősítéséről és az érintett tájékoztatásának szükségességéről az adatvédelmi tisztviselő hoz döntést.
42. **Adatvédelmi incidens:** lényegében a személyes adatok integritásának és bizalmas jellegének a sérülését jelenti. Az adatvédelmi tisztviselő részéről a NAIH-nak kötelezően bejelentendő.
43. **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.
44. **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).
45. **29-es Munkacsoport:** A 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosából, 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.

46. **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 bünyügyi igazságügyi adatkezeléseket szabályozó irányelv tervezetét.
47. **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 hatályba lép 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.
48. **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 elvesztett tulajdonnal, beutazási tilalmakkal kapcsolatos adatokat – úgynevezett figyelmeztető jelzéseket – helyeznek el a SIS-ben. Az érintettek SIS-sel kapcsolatos adatvédelmi kérésekkel (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.
49. **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.

50. **Cookie-k („sütit”):** 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. **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” hozzáállása az kell, hogy legyen, hogy minden körülmények között figyelembe veszik az adatvédelmi szempontokat és ezeknek megfelelően járnak el az adatkezelési műveletek során.