Nemzetközi Távközlési Adatvédelmi Munkacsoport

International Working Group on Data Protection in Telecommunications

Munkadokumentum: felhőalapú számítástechnika. A magánszféra és az adatok védelmének kérdései. „Sopot Memorandum".

*51. ülés – Sopot (Lengyelország), 2012. április 23-24.*[*]

**Tárgy**

Ebben a munkadokumentumban a személyes adatok feldolgozását tárgyaljuk különös tekintettel a felhő alapú számítástechnikai környezetre.

Nem vizsgáljuk azokat a helyzeteket, amelyekben minden végfelhasználó, adatfeldolgozó, adatkezelő és annak minden alvállalkozója ugyanazoknak az adatvédelmi jogszabályoknak az alanya, és telephelyük fizikailag ugyanazon a felségterületen van, és minden adatfeldolgozást és -tárolást ezen a felségterületen végeznek. A munkadokumentum ugyancsak kevésbé releváns, ha a felhőszolgáltatás e szolgáltatás felhasználójának teljes ellenőrzése alatt áll.

A munkadokumentum végül csak a felhőszolgáltatásoknak azon vállalkozások és hatóságok általi felhasználásával foglalkozik, amelyek a létező eljárásokat a „felhőben" végzik, és nem foglalkozik e szolgáltatás igénybevételével a magánszemélyek által.

**Általános háttér**

*„A felhő alapú számítástechnika egy fejlődésben lévő paradigma"*[1]

A felhő alapú számítástechnika iránt nő az érdeklődés, mert nagyobb gazdaságosságot, kisebb környezetterhelést, egyszerűbb működtetést ígér, barátságosabb a felhasználóhoz és számos egyéb előnnyel jár.

2011 szeptemberében a Nemzeti Szabványügyi és Technológiai Intézet (NIST) az SP 800-145 jelű speciális közleményében a felhő alapú számítástechnikát a következőképpen határozta meg:

> *„A felhő alapú számítástechnika egy olyan modell, amely széleskörű, kényelmes, igény szerint rendelkezésre álló hálózati hozzáférést kínál konfigurálható számítástechnikai erőforrásokhoz (pl. hálózatokhoz, szerverekhez, tárakhoz, alkalmazásokhoz és szolgáltatásokhoz), amelyek gyorsan és minimális kezelési ráfordítással és minimális, a szolgáltatóval folytatott interakcióval igénybe vehetők, és nyilvánosan rendelkezésre állhatnak. Ez a felhőmodell öt lényeges tulajdonságot tartalmaz, három szolgáltatási és négy felhasználási modellt."*[2]

Ez a meghatározás, egyebek mellett

---

[*] A Munkacsoport „Working Paper on Cloud Computing - Privacy and data protection issues – 'Sopot Memorandum'" című dokumentumának fordítása (Dr. Könyves-Tóth Pál munkája) figyelemmel német nyelvű változatára is. Letölthető: **http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group**

*„ .... annak megvitatására nyújt alapot, mi is az a felhő alapú számítástechnika, és hogyan használhatjuk azt a legjobban.”*[3]

A meghatározás elősegíti a felhő alapú számítástechnika jobb értelmezését. Ez az értelmezés jelenleg is gyorsan fejlődik. A NIST meghatározása kiváló kiinduló pont a felhő alapú számítástechnika további vizsgálatára és felhasználására.

Egyébként még mindig vannak tisztázatlan, a felhő alapú számítástechnikával kapcsolatos kérdések, különösen ami a magánszférát, az adatvédelmet és más jogi vonatkozásokat érint. A munkadokumentum ajánlásai segítenek e tisztázatlan kérdések számát csökkenteni.

Először is a javaslatokat soroljuk fel. A második rész további háttérinformációt tartalmaz a felhő alapú számítástechnikát illetően, és indokolja a javaslatokat. Aki közelebbről kíván a témával megismerkedni, az először ezt a részt olvassa.

E munkadokumentum céljára a felhő ügyfelének az adatkezelőt tekintjük, a felhőszolgáltatás nyújtójának pedig az adatfeldolgozót.[4]

A felhő alapú számítástechnikát egy sor fontos témát ölel fel, pl. a következőket:

a. nincs még nemzetközi megegyezés az egységes terminológiát illetően;
b. a technológia még mindig fejlődik;
c. óriási adatmennyiség halmozódik fel és koncentrálódik;
d. a technológia határtalan és határátlépő[5];
e. az adatfeldolgozás globálissá válik;
f. a felhőszolgáltatást nyújtók folyamatai, eljárásai és gyakorlata nem átláthatóak, ide értve azt is, hogy a felhőszolgáltatást nyújtók a feldolgozással alvállalkozót bíznak meg vagy nem, s ha igen, azok milyen folyamatokat, eljárásokat és módszereket alkalmaznak;
g. az átláthatóságnak ez a hiánya megnehezíti a kockázatok megfelelő értékelését;
h. az átláthatóságnak ez a hiánya következtében nehezebb az adatvédelmi szabályokat érvényesíteni;
i. a felhőszolgáltatást nyújtók nagy nyomásnak vannak kitéve, hogy gyorsan tőkésítsék magas befektetési költségeiket;
j. az ügyfelek, részben a világszerte jelentkező pénzügyi válság következtében növekvő nyomásnak vannak kitéve, hogy adatfeldolgozási költségeiket csökkentsék;
k. a felhőszolgáltatók, hogy áraikat csökkentsék, inkább általános szolgáltatási feltételeket kínálnak.

Ezek a körülmények **az alábbi, növekvő kockázatokkal járhatnak**:

A. az információ-biztonság áttörése, például a (személyes) adatok bizalmas voltának, integritásának vagy rendelkezésre állásának megsértése anélkül, hogy azt az adatkezelő észlelné;
B. az adatokat olyan felségterületekre továbbítják, amelyek az adatok védelmét nem megfelelően biztosítják;
C. az adatvédelmi jogszabályokat és alapelveket sértő cselekmények;

D. az általános szolgáltatási feltételeket alkalmazó adatkezelő túl sok játékteret enged meg a felhőszolgáltatás nyújtójának, ide értve azt a lehetőséget, hogy a felhőszolgáltatás nyújtója az adatokat az adatkezelő utasításait sértő módon dolgozza fel;
E. a felhőszolgáltatás nyújtója vagy alvállalkozója az adatkezelő adatait annak tudta és engedélye nélkül saját céljaira használja fel;
F. az elszámoltathatóság és felelősség az alvállalkozói láncban észrevehetően csökken vagy eltűnik;
G. az adatkezelő elveszíti az adatok és az adatfeldolgozás feletti ellenőrzését;
H. az adatkezelő vagy megbízható harmadik fele (pl. az auditor) képtelen megfelelően ellenőrizni a felhőszolgáltatás nyújtóját;
I. az adatvédelmi hatóságoknak nincs lehetőségük arra, hogy a személyes adatoknak az adatkezelő és a felhőszolgáltatás nyújtója által végzett feldolgozását megfelelően felügyeljék;
J. az adatkezelő a hiányos információk és felügyelet következtében potenciálisan megsérti a telephelyéül szolgáló ország hatályos adatvédelmi jogszabályait.

**A következő ajánlások hozzájárulnak a felhőszolgáltatások igénybevétele kockázatainak csökkentéséhez, és elősegítik felelősségteljes alkalmazásukat**[6], minek következtében a felhőszolgáltatások alkalmazásának előnyei érvényesülhetnek, de nem az egyén jogainak sérelmére.

## Ajánlások[7]

### Általános ajánlások

A Munkacsoport az alábbi ajánlásokat teszi:

- a felhő alapú számítástechnika, összevetve a hagyományos adatfeldolgozással, nem vezethet az adatvédelmi szabályok gyengítéséhez;
- az adatkezelők, mielőtt hozzákezdenek egy felhő alapú számítástechnikai projekt megvalósításához, végezzék el a szükséges adatvédelmi hatás- és kockázat-elemzéseket (esetleg egy bizalmi harmadik fél segítségével);
- a felhőszolgáltatások nyújtói folyamatosan fejlesszék eljárásaikat a nagyobb átláthatóság, biztonság, ellenőrizhetőség és bizalom növelése érdekében, különös tekintettel az adatok esetleges sérelmére és a kiegyensúlyozottabb szerződési feltételekre vonatkozó információkra, ily módon támogatva az adatoknak a felhőszolgáltatások igénybevevői általi hordozhatóságát és ellenőrizhetőségét;
- tovább kell folytatni a kutatásokat, fejleszteni kell a harmadik fél általi tanúsítást, a szabványosítást, a ”beépített adatvédelmi” és más, ezzel összefüggő technológiákat, hogy felhő alapú számítástechnikával szemben megkívánt bizalmi szintet elérjék;
- a jogalkotók vizsgálják felül, hogy a határátlépő adattovábbításra vonatkozó jogszabályok továbbra is érvényesek-e, és fontolják meg, szükség van-e újabb adatvédelmi biztosítékokra a felhő alapú számítástechnika korszakában[8];
- a magánszféra- és adatvédelmi hatóságok folyamatosan informálják az adatkezelőket, a felhőszolgáltatások nyújtóit és a jogalkotókat a magánszféra- és adatvédelmi kérdésekről.

### További útmutatás a legjobb gyakorlatokra („best practices”)

1. a felhőalapú számítástechnika alkalmazását gondos, mértéktartó lépésekben kell végrehajtani, kezdve a nem különleges és nem bizalmas adatokkal;

2. a különleges[9] adatok felhőalapú feldolgozása újabb aggodalmakat kelt. Ezért az ilyen feldolgozásra vonatkozó nemzeti jogszabályokba, azok sérelme nélkül, további biztosítékokat kell beépíteni;

3. **A helykövető ellenőrzési nyomvonal** adatait hozzáférhetővé kell tenni az adatkezelő és az adatvédelmi hatóságok számára. Az **ellenőrzési nyomvonalat** automatikusan rögzíteni kell, és mutatnia kell azt a fizikai helyet és időpontot, ahol és amikor a személyes adatokat tárolják vagy feldolgozzák[10].

4. Egy **automatikusan rögzített másoló és törlő ellenőrzési nyomvonalat** kell létrehozni, amely világosan mutatja, hogy a személyes adatok másolatát a feldolgozó vagy alvállalkozója hozta létre vagy törölte.

5. A helykövető **ellenőrzési nyomvonalnak** és a másoló vagy törlő **ellenőrzési nyomvonalaknak** az adatbiztonságról is gondoskodniuk kell.

6. Hatékony technikai intézkedéseket kell kifejleszteni, amelyek a személyes adatok jogellenes továbbítását elégséges adatvédelemmel nem rendelkező felségterületekre megakadályozzák.

7. Biztosítani kell, hogy a személyes adatokat a lemezekről és más tároló eszközökről ténylegesen **töröljék**, pl. azoknak **véletlen adatokkal való haladéktalan felülírásával**[11].

8. Biztosítani kell, hogy a nem használt és a továbbított adatokat elismert szabványos algoritmusokkal és aktuális kulcshosszúsággal **kódolják**[12]. A kódoló kulcsot senki más nem használhatja vagy férhet ahhoz hozzá, mint az adatkezelő és a felhőszolgáltatást nyújtó. A kulcsot csak a felhőszolgáltatást nyújtó ügyfelei használhatják vagy férhetnek ahhoz hozzá. Az adatok nem kódolt formában csak addig és csak nem nagyobb terjedelemben férhetők hozzá, ameddig arra a mindenkori adatfeldolgozáshoz feltétlenül szükség van. Újabb módszereket kell kidolgozni, amelyek segítségével az adatok a felhőszolgáltatás nyújtójának olvashatatlanná tehetők[13]. Hasznos lehet olyan lehetőségek felkutatása, melyekkel az adatkezelő az adatok kódolásának feloldását hatékonyan és gyorsan elvégezheti (vészfék).

9. A személyes adatoknak, minden, a felhőszolgáltatást nyújtó általi felhasználását automatikusan **jegyzőkönyvezni** kell. A jegyzőkönyvet egyszerű, könnyen érthető formában, könnyen hozzáférhetővé kell tenni az adatkezelő számára. A felhőszolgáltatást nyújtónak és alvállalkozójának biztosítania kell a jegyzőkönyv integritását.

Az adatkezelő

10. Az adatkezelőnek a felhőszolgáltatás nyújtójával meg kell állapodnia egy teljes listában, amely minden fizikai helyre vonatkozó információt tartalmaz, ahol a megállapodás futamidejében a felhőszolgáltatást nyújtó és/vagy alvállalkozója adatokat tárol vagy dolgoz fel, ide értve az adatbiztonságot is (**a hely átláthatóságának alapelve**).

11. E megállapodásban az adatkezelőnek biztosítania kell, hogy sem a felhőszolgáltatást nyújtó, sem alvállalkozói nem továbbítanak más helyekre adatokat, csak a megállapodásban rögzített listában feltüntetett fizikai helyekre, tekintet nélkül a továbbítás indokára és arra, hogy az adatok kódolva vannak-e vagy sem. Ezt technikai intézkedésekkel is támogatni kell, melyek fennállásáról és megbízhatóságáról az adatkezelő ténylegesen meggyőződhet.

12. Az adatkezelőnek biztosítania kell, hogy a felhőszolgáltatás nyújtójával kötött megállapodás nem félreérthető és nem ad lehetőséget olyan értelmezésekre, amelyek aláássák azt az elvet, hogy a felhőszolgáltatás nyújtója csak az adatkezelő utasításai szerint dolgozhat fel személyes adatokat. Ha a felhőszolgáltatás nyújtója egyoldalúan megváltoztatja a megállapodást, az adatkezelőnek legyen joga arra, hogy felbontsa a megállapodást, és az adatokat másik felhőszolgáltatás nyújtónak továbbítsa.

13. A megállapodásban kifejezetten ki kell kötni, hogy a felhőszolgáltatás nyújtója az adatkezelő adatait nem használhatja fel saját céljaira.

14. Az adatkezelőnek legyen lehetősége megvizsgálni vagy megvizsgáltatni minden olyan helyszínt, ahol részben vagy egészben személyes adatokat dolgoznak fel jelenleg, dolgoztak fel a múltban vagy dolgoznak fel a megállapodás szerint a jövőben. A megállapodásban ki kell kötni, hogy az adatfeldolgozó joga részletesen betekinteni a felhőszolgáltatás nyújtója és alvállalkozói minden olyan tevékenységébe, melyet szükségesnek tart a megállapodással való összhang szempontjából, ide értve annak biztosítását is, hogy a személyes adatok feldolgozását az utasítások szerint, jogszerűen és megfelelő biztonsággal végzik.

15. A megállapodásban az adatkezelőnek biztosítani kell egy megbízható harmadik félnek (pl. egy elismert auditáló cég)[14] azt a jogát, hogy teljes egészében vagy részben nyomon kövesse, hogy a felhőszolgáltatás nyújtója vagy alvállalkozói, ha vannak, hogyan dolgozzák fel a személyes adatokat.

16. A felhőszolgáltatás igénybe vételét megelőzően az adatkezelőnek el kell végeznie azoknak a különös feltételeknek és körülményeknek a **kockázatelemzését,** melyek közepette a felhőszolgáltatás nyújtója vagy, ha van ilyen, alvállalkozója az adatokat feldolgozza. A kockázatelemzésnek ki kell terjednie minden olyan helyszínre, ahol személyes adatokat dolgoznak fel vagy tárolnak.

17. Az adatkezelőnek a kockázatelemzést rendszeresen felül kell vizsgálnia és frissítenie kell mindaddig, amíg a felhőszolgáltatás nyújtója a személyes adatokat feldolgozza.

18. A felhőszolgáltatás igénybevételét megelőzően az adatkezelőnek gondoskodnia kell arról, hogy a felhőszolgáltatásból való kilépésre tényleges lehetősége legyen, ide értve a felhőszolgáltatást nyújtó aktív szerepét az adatok az adatok továbbítása tekintetében, hogy magát egy felhőszolgáltatás nyújtójától függetlenítse (lock-in effektus).

19. Az adatkezelőnek meg kell fontolnia, szükséges-e annak biztosítása, hogy az adatok legalább egy használható másolata hozzáférhető legyen a felhőszolgáltatást nyújtó (és alvállalkozói) ellenőrzése, hozzáférhetősége vagy befolyásolása nélkül. Ha

szükségesnek látszik, a másolatnak, a felhőszolgáltatás nyújtójától és alvállalkozói részvételétől függetlenül, hozzáférhetőnek és felhasználhatónak kellenie.

20. Az adatvédelmi szabályok megszegése esetén az adatkezelőnek képesnek kell lenni kötelezettségei teljesítésére mind az adatalanyt, mind az adatvédelmi hatóságokat illetően, és meg kell tennie a megfelelő intézkedéseket. E tekintetben az adatkezelőnek világos megállapodást kell kötnie a felhőszolgáltatás nyújtójával, hogy az adatvédelmi rendelkezések efféle megsértése esetén azonnal és minden részletre kiterjedően értesíthesse az adatkezelőt és az adatvédelmi hatóságot.

21. Az adatkezelőnek a felhőszolgáltatás nyújtójával kötött megállapodásban kötelezniе kell a szolgáltatót, hogy hatékony és azonnali eljárásokat alkalmazzon annak érdekében, hogy az adatalanyok gyakorolhassák az adatokhoz való hozzáférés, helyesbítés, törlés vagy zárolás jogát.

A felhőszolgáltatás nyújtója

22. A felhőszolgáltatás nyújtójának gondoskodnia kell arról, hogy az adatkezelő teljes átláthatósággal rendelkezzék azokról a helyszínekről, ahol a felhőszolgáltatás nyújtója vagy, ha van ilyen, alvállalkozói személyes adatokat dolgoznak fel vagy tárolnak.

23. A felhőszolgáltatás nyújtójának biztosítania kell, hogy alvállalkozói tevékenysége és az általuk végzett adatfeldolgozási folyamatok tökéletesen átlátszók legyenek.

24. A felhőszolgáltatás nyújtójának a szerződés tárgyában átláthatóságról kell gondoskodnia, és a felhőszolgáltatás nyújtójának nem kínálhat olyan szerződéses feltételeket, amelyek a szerződés egyoldalú módosítását teszik lehetővé.

25. A felhőszolgáltatás nyújtóját és – ha van ilyen – alvállalkozóit arra ösztönözzük, hogy kövessék a legjobb gyakorlatot, és tegyék lehetővé, hogy egy pártatlan harmadik fél teljesítményüket összehasonlítsa és értékelje (benchmarking).

26. Bizonyos piaci szegmensek, pl. kis és közepes vállalkozások részére az általános szerződési feltételeket magánszféra és a megfelelő védelmi intézkedések figyelem vételével kell kialakítani.

Auditálás

27. Minthogy egy felhőszolgáltatást nyújtó nagy tömegű személyes adatot tud gyűjteni, a felhőszolgáltatás a felhőszolgáltatás nyújtóját az adatkezelőt saját érdekében az általa végzett auditot követően alá kell vetni egy harmadik fél által végzett auditnak. Az auditornak teljesen függetlennek kell lennie a felhőszolgáltatás nyújtójától, és különös figyelmet kell fordítania a személyes adatok feldolgozásának biztonságára. Az auditornak különösen azt kell megvizsgálnia, hogy megtették-e az intézkedéseket a következő területeken, és azok megfelelően működnek: helykövető **ellenőrzési nyomvonal** (vö.: 3. pont), másolási és törlési **ellenőrzési nyomvonal** (vö.: 4. pont), törlés (vö.: 7. pont) és jegyzőkönyvezés (vö.: 9. pont). Az auditornak továbbá ellenőriznie kell, hogy a következő intézkedéseket megtették-e, s hogy azok megfelelően működnek: intézkedések az adatok megfelelő adatvédelmi szabályokat nélkülöző felségterületekre való jogellenes továbbításának megakadályozására (vö.: 6.

pont), és intézkedések annak érdekében, hogy az adatokat az ügyfél kifejezett hozzájárulása nélkül egyéb helyszínekre ne továbbítsák (vö.: 10. és 11. pont). Végül az auditornak biztosítania kell, hogy ezeket az intézkedéseket sem a felhőszolgáltatás nyújtója, sem – ha van ilyen – alvállalkozója észrevétlenül nem sértheti meg.

**Az ajánlások háttere**

28. A felhőalapú számítástechnika az adatfeldolgozás **új paradigmája**, amelyre – jobb megnevezés hiányában – mint **hagyományos adatfeldolgozásra** hivatkozunk. A hagyományos adatfeldolgozást tekintve hosszú évek során jelentős tapasztalatokra tettünk szert, míg a felhőalapú számítástechnikával kapcsolatban hasonló jelentős tapasztalataink nincsenek.

29. E **paradigmaváltás** következménye, hogy az adatfeldolgozás alapvető feltételei, tapasztalatai, ideái, elméletei és modelljei már nem egyeznek meg a gyakorlattal, és ezért ezért mindezeket kritikai megfontolás, újraértékelés és adott esetben átdolgozás alá kell vetni. Ez a magánszféra és a személyes adatok védelmére, továbbá arra is vonatkozik, hogyan analizálhatjuk, értékelhetjük és ítélhetjük meg a **kockázatokat**. Ami tegnap a legjobb gyakorlat volt, manapság nem szükségképpen a legjobb gyakorlat.

30. Ezt az **új helyzetet** meg kell vizsgálni és **gondosan megválasztott lépésekben** kell kezelni, különös tekintettel a magánszféra és az adatok védelmére, valamint- szélesebb értelemben – az adatalany jogaira nézve.

31. A felhőalapú számítástechnika **technikai alapja** egy jól kifejlesztett hálózati technológia és szervervirtualizálás. Ez lehetővé teszi az adatok és az adatfeldolgozás dinamikus áttelepítését a mindenkori számítóközpont szerverei között lokálisan, valamint globálisan a világszerte működő számítóközpontok szerverei között. A technológia jól méretezhető anélkül, hogy az korlátozó szűk keresztmetszeteket hozna létre. Az Internet lehetővé teszi, hogy a végfelhasználó a számítóközpont telephelyétől függetlenül az adatokhoz hozzáférjen.

32. A felhőalapú számítástechnika **gazdasági hajtóereje a méretgazdaságosság**. Az adatfeldolgozás nagy központokba való koncentrálása javítja a drága erőforrások felhasználását, pl. az emberi tudását, a tárgyi tőkéjét (hardver, szoftver, épületek), a kommunikáció sávszélességét és az energiáját. Ezen túlmenően a felhőalapú szolgáltatások nyújtói nagyságuk és tömegük következtében, amikor erőforrásokat vásárolnak, különösen erős a tárgyalási pozíciójuk. A felhőszolgáltatások nyújtói ezért csökkenthetik darabonkénti költségeiket, és kedvezőbb egységárakat kínálhatnak ügyfeleiknek. A méretgazdaságosság elérésének feltétele, hogy sok ügyfél legyen az „áruházban”. Egy kielégítő **tömeg** elérése érdekében a felhőalapú szolgáltatásokat világszerte az Interneten kínálják.

33. A felhőalapú számítástechnika nagy lehetőséget kínál a kis és közepes vállalkozásoknak arra, hogy hozzáférjenek a megfizethető árú és méretezhető számítástechnikai forrásokhoz. A viszonylag nagy számú kisebb szervezetek arra számítanak, hogy a felhőszolgáltatás nyújtói e piaci szegmens részére általános szerződési feltételek dolgoznak ki.

34. A felhőalapú számítástechnika sokkal dinamikusabb, mint a hagyományos adatfeldolgozás. Az adatfeldolgozás helyszíne drámaian megváltozhat. Az adatok és feldolgozásuk aktuális helyszíne ugyanis számos olyan tényezőtől függhet, melyekre a végfelhasználók és adatkezelők hagyományosan kevés figyelmet fordítottak és e tényezőket nem feltétlenül tekintik át vagy nem képesek őket kontrollálni. A felhőalapú szolgáltatások nyújtói például gyakran több országban telepítenek adatközpontokat, figyelembe véve többek között az olcsó a villamosenergiát, a hűvös helyi időjárást és az időzónát. Előre nem látható körülmények is hatással lehetnek az adatok aktuális helyszínére, így például akkor, ha egy adatközpont leáll, vagy csúcsterhelés esetén a kapacitás hiánya miatt (túlcsordulás). Ekkor – egy adatközpont leállása esetén vagy biztonsági másolatok céljából – az adatok másolatait más adatközpontokba lehet továbbítani (redundancia).

35. A felhőalapú számítástechnikát számos ügyfél veszi igénybe, akik a felhőalapú szolgáltatások forrásait egymás közt megosztva használják. Ez azonban csak akkor következhet be, ha a felhőalapú szolgáltatások egyes igénybevevőinek adatai és azok feldolgozása **világosan elkülöníthető**. A források megosztása az adatok tömeges elvesztésével vagy illetéktelen felfedésével járhat.[15] A kockázat azáltal is növekszik, hogy a felhőszolgáltatás nyújtója a költségek optimalizálása céljából nagy tömegű adatot kezel (méretgazdaságosság). A felhőszolgáltatás nyújtójának ügyfelei egymásnak is kockázatot jelentenek. Minél több ügyfél osztozik ugyanazokon a forrásokon, annál nagyobb kockázat minden egyes ügyfél számára, és ezáltal a felhőszolgáltatás valamennyi ügyfelének.

36. A felhőalapú számítástechnika és kockázatainak ismerete jelenleg viszonylag kis számú nagy felhőalapú szolgáltatás nyújtó körében összpontosul, akik kereskedelmi és versenyképességi okokból vonakodnak attól, hogy széleskörű betekintési lehetőséget adjanak a specifikus feltételekbe és körülményekbe. Az ismeretek és a betekintési lehetőségek egyenlőtlen megoszlása a felhőszolgáltatások nyújtói és ügyfeleik között ez utóbbiakat gyenge helyzetbe hozza, amikor megállapodást akarnak kötni, és megnehezíti, hogy megfelelően értékeljék a felhőalapú szolgáltatások igénybevételével kapcsolatos kockázatokat.

37. Egy alapos **kockázatelemzésnek** a felhőszolgáltatás tényleges szerkezetének **ismeretén** és a felhőszolgáltatás valamennyi, olyan helyszínének körülményein kell alapulnia, ahol adatokat dolgoznak fel.

38. A felhőalapú számítástechnika **határtalan** és **átnyúlik a határokon**. A globális ügyfélkör a felhőalapú adatközpontok globális ügyfélkörével és az adatok dinamikus mozgásával együtt azt eredményezhetik, hogy az adatok átlépik a nemzeti határokat és különféle felségterületekre kerülnek, ahol hiányzik a megfelelő átláthatóság. A személyes adatok megfelelő adatvédelemmel nem rendelkező felségterületek adatközpontjaiba kerülhetnek, kereskedelmi célra visszaélhetnek velük vagy idegen hatalmak számára jogosulatlanul hozzáférhetővé válnak.[16]

39. Az adatvédelmet tekintve meg kell különböztetni az adatkezelő és a feldolgozó egymás kölcsönösen kizáró szerepét. **Adatkezelő** az, aki meghatározza az adatfeldolgozás célját és módját az adatfeldolgozás egy maghatározott folyamatában.

40. Széles körben elfogadott az is, hogy egy adatkezelő megengedheti a személyes adatok feldolgozásának egy **feldolgozó** által való végzését, de csak a kezelő kifejezett **utasításai** szerint.

41. Általánosan elismert adatvédelmi elv, hogy a feldolgozó nem dolgozhat fel nagyobb terjedelemben személyes adatokat, csak az adatkezelő kifejezett utasításai[17] szerint. Ez a felhőalapú szolgáltatás esetében azzal jár, hogy a felhőalapú szolgáltatás nyújtója nem hozhat egyoldalú döntést, vagy nem engedheti meg a személyes adatok automatikus továbbítását (vagy feldolgozását) ismeretlen adatközpontokba. Ennek attól függetlenül is így kell lennie, hogy a felhőalapú szolgáltatás nyújtója egy ilyen továbbítást azzal igazol, hogy így csökkenti a működtetés költségeit, kezelni képes a csúcsterhelést (túlcsordulást), a terhelés elosztását, a biztonsági másolatok készítését, stb. A felhőszolgáltatás nyújtója nem használhatja fel a személyes adatokat saját céljaira.[18]

42. Egy másik, általánosan elismert adatvédelmi elv megköveteli, hogy az adatkezelő megfelelő **technikai és szervezési intézkedéseket** foganatosít annak érdekében, hogy az adatokat megvédje a véletlen vagy jogellenes megsemmisítésétől, elvesztésétől vagy megkárosításától, valamint illetéktelen közzétételétől vagy más, a jogszabályi rendelkezéseket sértő feldolgozásától. Mindez a feldolgozókra is vonatkozik.

43. Az adatkezelők felelősségének teljesítése megköveteli, hogy az adatkezelő **nyomon követi** a feldolgozó által végzett feldolgozást annak biztosítása érdekében, hogy az összhangban legyen az adatkezelő utasításaival, és a feldolgozást megfelelő biztonsággal végzik.

44. Felelősségének sérelme nélkül az adatkezelő kifejezett utasításokat adhat, hogy a feldolgozó által végzett feldolgozást részben egy **megbízható harmadik fél** (pl. az auditor) végezze. Ennek feltétele, hogy a harmadik fél a szükséges képzettséggel rendelkezzék, független legyen a feldolgozótól, hozzáférjen és betekintsen azokba az aktuális feltételekbe és körülményekbe, melyek alapján a feldolgozó a feldolgozást végzi, és megbízható jelentést adjon megfigyeléseiről, értékelésétől és következtetéseiről az adatkezelőnek.

A Munkacsoport továbbra is figyelemmel kíséri a felhőalapú számítástechnika fejlődését, és – ha szükséges – frissíti ezt a munkadokumentumot.

---

[1] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, 2011. szeptember, 2. oldal.

[2] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, 2011. szeptember, 3. oldal.

[3] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, 2011. szeptember, 2. oldal.

[4] Lásd lentebb a 39, és 40. bekezdést. A felhőszolgáltatás nyújtójának alvállalkozóját a személyes adatok feldolgozásával kapcsolatban ugyancsak feldolgozónak tekintjük.

[5] Lásd 35. bekezdés.

[6] Az ENISA a „Cloud Computing – Benefits, risks and recommendations for information security” (Felhő alapú számítástechnika – előnyök, kockázatok és ajánlások) címen 2009. novemberében közzétett jelentésének 9-10. oldalán felsorolja a leggyakoribb biztonsági kockázatokat, melyek a következők: véletlenszerű sorrend, az ellenőrzés elvesztése, egy szolgáltatásnyújtótól való függés (Lock-in-Effekt), az adatok nem biztonságos vagy nem teljes törlése, hibás elkülönítés, adatvédelem, rosszindulatú beavatkozás. További részletek a jelentésben olvashatók. Ehelyütt az ellenőrzés elvesztését hangsúlyoztuk.

[7] Az ajánlások listája nem teljes.
[8] Vö.: Adat- és Magánszféravédelmi Biztosok Nemzetközi Konferenciája: A Személyes Adatok és a Magánszféra Védelmére hivatott Nemzetközi Szabványok („Madridi Határozat"), 2009 november 5. **http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf**
[9] A különleges adatok koncepciójának az egyes jogi kultúrákban eltérő a jelentése, vö. 95/46/EK irányelv 8. cikk, Általános Adatvédelmi Rendelettervezet, 9. cikk, és az FTC Jelentés „Protecting Consumer Privacy in an Era of Rapid Change" (2012).
[10] A helykövető **ellenőrzési nyomvonal** például világos áttekintést adhat arról, mikor rögzítették vagy törölték az egyes helymeghatározó személyes adatokat, s hogy azokat hová, mely helyre továbbították.
[11] Az adatok törlése referenciájuktól való megfosztásukkal, és későbbi felülírásuk a tárterület ismételt igénybevételével általában nem elégséges, mert továbbra is fennáll annak lehetősége, hogy az adatok a tárterület újbóli igénybevételével a megújult referencia által ismét hozzáférhetővé válnak.
[12] Az adattovábbítás során egy végtől-végig kódolást kell alkalmazni. Biztosítani kell, hogy a továbbított személyes adatok védve vannak az aktív (pl. Replays, Traffic Injection), és a passzív (pl lehallgatás) támadásoktól. Továbbá a nem használt adatokhoz való hozzáférést illetéktelen felektől megfelelő technikai és szervezési eljárásokkal meg kell akadályozni (pl. hozzáférés-ellenőrzéssel, az adatok kódolásával).
[13] Az e területen folyó kutatás egy példája a lepecsételt felhő (Sealed Cloud) kezdeményezés, melyről Hubert Jäger und Arnold Monitzer egy cikk tervezetét „Sealed Cloud - a novel approach to defend insider attacks" címen tette közzé. Lásd: **http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf**
[14] A megbízható harmadik félről részletesebben lásd a 44. pontot.
[15] Az ENISA a *Cloud Computing – Benefits, risks and recommendations for information security (Felhőalapú számítástechnika: előnyök, kockázatok, és információbiztonsági ajánlások) címen 2009. novemberben közzétett* jelentésében véletlenszerű sorrendben felsorolja a legjelentősebb kockázati tényezőket: az ellenőrzés elvesztése, egyetlen szolgáltatótól való függőség (lock-in effektus), elkülönítési hiba, adatvédelem, nem biztonságos vagy hiányos adattörlés vagy belső támadó. További részletek a jelentésben olvashatók. Itt hangsúlyoznunk kell, hogy a legjelentősebb kockázat az elkülönítési hiba.
[16] Ámbár a személyes adatok feldolgozása egyetlen felségterületen zajlik, a felhőszolgáltatás nyújtója vagy anyavállalata egy másik felségterületen is elhelyezkedhet, ily módon lehetővé téve a külföldi bűnüldöző szerveknek a felhőszolgáltatás adataihoz való hozzáférést akkor is, ha az adatokat fizikailag ennek az országnak a földrajzi határain kívül tárolják. E kérdés szabályozására egy nemzetközi szerződés válhat szükségessé.
[17] Vagy jogszabály alapján.
[18] Ha a felhőszolgáltatás nyújtói az adatkezelő tudta nélkül dolgoznak fel személyes adatokat, a felhőszolgáltatás nyújtóját társfeldolgozónak kell tekinteni, s mint ilyen, felelős az adatoknak a felhatalmazást nélkülöző, független feldolgozásáért.