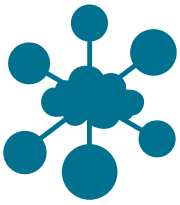
CLOUD COMPUTING MAGYARORSZÁGON

A JOGI SZABÁLYOZÁS



TARTALOM

Előszó	4
Hogyan használja ezt a kiadványt?	5
A kérdőíves alfejezetekben használt fogalmak	6
Cloud computing – rövid technikai áttekintés jogi szakemberek számára	7
Cloud computing és adatvédelem	14
Általános követelmények	20
Magyarország	31

ELŐSZÓ

Örömünkre szolgál, hogy bemutathatjuk Önnek a Cloud Computing Magyarországon – a jogi szabályozás című kiadványt.

Ez a kiadvány a legfontosabb jogi témákat ismerteti olyan jogi szakemberek és üzletemberek számára, akik Magyarországon cloud computing termékekkel és szolgáltatásokkal kerülnek kapcsolatba.

Ezt a tanulmányt a Cseh Köztársaságban, Prágában működő, a számítástechnika területére szakosodott jogi iroda, a PIERSTONE szakértői csoportja készítette és koordinálta.

A Cloud Computing – Műszaki áttekintés jogi szakemberek számára című cikket egy szintén Prágában, a Cseh Köztársaságban dolgozó független cloud computing szakértő, Zdenek Jirícek írta.

Szeretnénk köszönetünket nyilvánítani Dr. Jochen Engelhardt úrnak, a Microsoft jogi és társasági ügyek közép- és kelet-európai jogi igazgatójának, akitől ennek a kiadványnak az ötlete származik, és aki annak megvalósításához is jelentős támogatást nyújtott.

A szerkesztők: Lenka Suchánková, partner (lenka.suchankova@pierstone.com) és Jana Pattynová, partner (jana.pattynova@pierstone.com), PIERSTONE.

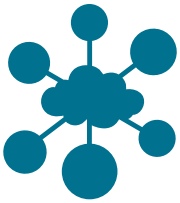
HOGYAN HASZNÁLJA EZT A KIADVÁNYT?

Ez a kiadvány négy részből áll.

A tanulmány első részében két cikk található, amelyek a felhő alapú számítástechnikát (röviden: számítási felhő, illetve cloud computing) technikai, valamint jogi szempontból tárgyalják, amelyeket a kiadvány kérdés-felelet részében használt fogalmak meghatározása egészít ki. Ezeket a bevezetésként szolgáló fejezeteket egy, az EU személyes adatok védelméről szóló általános jogszabályait a cloud computing szempontjából áttekintő rész követi, kérdések és válaszok formájában. A kiadvány záró részében egy kérdőív található, amely a cloud computing szempontjából releváns főbb magyar jogi követelményeket ismerteti.

A magyarországi szabályozást kérdés-felelet formában bemutató fejezet célja az uniós adatvédelmi szabályozástól való lényeges különbségeknek a kiemelése, amelyet mindig az EU általános adatvédelmi szabályozásáról szóló, hivatkozási alapként szolgáló ismertetéssel kell együtt olvasni.

Megjegyzés: Jelen kiadvány csakis tájékoztatásnak tekinthető. A kiadványban szereplő információk csak a cloud computing egyes aspektusaira vonatkozóan nyújtanak általános tájékoztatást. Nem ölelik fel ennek a szakmai területnek a teljességét: sem valamennyi kérdést, sem a tárgyalt témák kimerítő ismertetését. Jelen kiadvány időről időre hatályosításra kerülhet. Egy-egy eset specifikus körülményeire figyelemmel a jogszabályok alkalmazása és hatása jelentősen eltérő lehet. A szolgáltatott információk nem minősülnek hivatalos jogi tanácsnak, és azok nem helyettesíthetik jogi szakértővel folytatott konzultációt. Egy-egy döntés meghozatala, vagy jogi értékelést igénylő intézkedés előtt érdemes jogi szakértő véleményét kérni.



A KÉRDŐÍVES ALFEJEZETEKBEN HASZNÁLT FOGALMAK

Felhő Vélemény	Az EU 29. cikk szerinti adatvédelmi munkacsoport 05/2012 számú véleménye (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).
Az EU Adatvédelmi Rendeletének Tervezete	A 2013. január 16-án kelt javaslat az Európai Parlament és a Tanács rendeltére a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (Általános Adatvédelmi Rendelet) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65784/20130508ATT65784EN.pdf).
Adatvédelmi Hatóság	Az illetékes tagállami adatvédelmi hatóság.
EGT	Európai Gazdasági Térség.
Az EU Adatvédelmi Irányelve	Az Európai Parlament és a Tanács 95/46/EK (1995. október 24.) irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT).
EU Általános Szerződési Feltételek	Az Európai Bizottságnak a 95/46/EK irányelv alapján hozott, 2010. február 5-én kelt döntése a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről. (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF).
EU-US Biztonságos Kikötő Keretszabályok	Az Európai Bizottságnak az Európai Parlament és a Bizottság 95/46/EK számú irányelve alapján 2000. július 6-án hozott határozata az Egyesült Államok Kereskedelmi Minisztériuma által kiadott ‘Biztonságos Kikötő’ (Safe Harbor) adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos, gyakran felvetődő kérdésekről. (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML).
Személyes Adat	Az EU Adatvédelmi Irányelv 2. cikk a) pontjának meghatározása szerint értendő.
WP 29	Az EU Adatvédelmi Irányelv 29. cikke alapján létrehozott adatvédelmi munkacsoport.

CLOUD COMPUTING – RÖVID TECHNIKAI ÁTTEKINTÉS JOGI SZAKEMBEREK SZÁMÁRA

BEVEZETÉS

A cloud computing hatalmas jelentőségű paradigmaváltást jelent abban a tekintetben, hogy a számítástechnikai erőforrások miképpen érhetők el az egyes szervezetek és végfelhasználók számára. Saját hardver berendezéseik és szoftver felhasználási engedélyeik megvásárlása helyett a szervezetek ettől kezdve választhatnak, hogy azok mely részeit vagy szintjeit tartják saját tulajdonban, melyeket bérlik, és milyen szerződési feltételek szerint.

A legegyszerűbb párhuzam, amely az embernek eszébe jut, az elektromos energiaellátás példája. Mintegy kétszáz évvel ezelőtt, az első és a második ipari forradalom közötti átmenet idején, a gyárak még saját villanyáram-fejlesztő gőzturbináik segítségével látták el magukat. Később az olcsóbb és megbízhatóbb tömeges villanyáram-fejlesztés felváltotta az egyéni áramfejlesztőkkel való áramellátást. Az energia piaca szabályozott iparággá fejlődött, amelyet a villanyáramra különböző árazási metódusokat alkalmazó elektromos társaságok versengése mozdított előre, és amely tipikusan különválik az elektromos gerinchálózat működtetésétől. Úgy látszik, gazdaságos az elektromos áramnak a nemzeti határokon átívelő kereskedelme akkor is, ha ahhoz meg kell oldani bizonyos műszaki különbözőségek összehangolását (mint amilyen az ún. fázis átalakítók szükségessége).

Hasonlóképpen, a számítástechnikai erőforrásokat gazdaságosabban és nagyobb rugalmassággal lehet ajánlani a játéktér egy olyan szintjén, ahol a szereplők számítástechnikai szolgáltatásaikat felhőhöz hasonlítható infrastruktúrákon keresztül, tipikusan internet kapcsolódás révén nyújtják. A cloud computing lehetséges előnyei óriásiak. Ebbe beleértendő az informatikai rendszerek testre szabásának és magasabb szintre emelésének lehetősége a szervezetek egyedi szükségletei szerint, és az eddigieknél jóval szélesebb hozzáférés olyan számítástechnikai erőforrásokhoz, amelyeket korábban csak a valóban legnagyobb, globális társaságok használhattak. Ezen túlmenően, a ‘bárhol és bármikor’ való hozzáférés révén a közös munka lehetősége a világ bármely pontján lévő informatikai felhasználók számára elérhetővé vált, és az új informatikai paradigma lehetőségei felé tömegesen forduló fejlesztők számára új lehetőségek nyíltak meg az újításokra. Kiváltképpen kormányzatok és hatóságok számára nyújt a cloud computing lehetőséget a költségeik csökkentésére gazdasági megszorítások idején is, mialatt az adatokhoz a polgárok könnyebben férhetnek hozzá, és a kormányzás átláthatóvá tételének ügye is kedvezően alakulhat.

A CLOUD COMPUTING LÉNYEGI ISMÉRVEI

A NIST[1] meghatározás szerint a cloud computing a felhőszolgáltató által kínált „olyan modell, amelynek révén a felhasználók kényelmesen és igény szerint férhetnek hozzá a megosztott, beállítható informatikai erőforrásokhoz, amelyeket gyorsan és minimális adminisztrációs megterhelés vagy szolgáltatói beavatkozás mellett rendelkezésre lehet bocsátani és fel lehet szabadítani”. Öt lényeges jellemzője van:

- **Igény szerinti önkiszolgálás:** az ügyfél rendszergazdája automatikusan nyújtani tudja a számítástechnikai erőforrást anélkül, hogy a szolgáltatóval személyes kapcsolatot kellene létesíteni.
- **Széles hálózati hozzáférés:** a hálózaton különböző féle ügyfélplatformok (PC-k, táblagépek, okostelefonok) hozzáférése lehetséges az erőforrásokhoz.
- **Erőforrás megosztás:** a felhőszolgáltató erőforrásai nagy számú felhasználó számára állnak rendelkezésre egy több-bérlős modellben, mialatt a fizikai és virtuális források dinamikusan hozzárendelhetők a felhasználói igényekhez.
- **Gyors rugalmasság:** az erőforrások bővítése vagy csökkentése olyan sebességgel történik, hogy azok a felhasználó számára korlátlannak és bármikor elérhetőnek látszanak.
- **Mérhető szolgáltatási mennyiség:** a forrásfelhasználás mérhető, miközben mind a szolgáltató, mind a felhasználó számára átlátható.

FELHŐSZOLGÁLTATÁS-NYÚJTÁSI MODELLEK

Két elsődleges ismérv használatos a különféle szolgáltatás-nyújtási modellek osztályozásához: a hely, ahol a szolgáltatás fut (a felhasználó működési helye vagy a felhőszolgáltató adatközpontja) és a hozzáférés szintje (megosztott, vagy egyetlen szervezet rendelkezésre áll).

- **Magán felhő (private cloud).** A felhő infrastruktúra egyetlen szervezet vagy vállalkozás rendelkezésére áll, amely számos felhasználói csoportot foglalhat magában (pl. üzleti egységeket). Tulajdonosa és üzemeltetője vagy a szervezet maga, vagy pedig harmadik személy. Ha a rendelkezésre bocsátott erőforrások hosztoltak, akkor a magán felhő egy sajátos típusáról van szó: ez a ‘hosztolt magán felhő’. Példák erre: az IT részleg képes a HR, a pénzügyek , a számvitel és az üzletviteli alkalmazások futtatására egyazon telephelyen belül teljesen virtualizált, közös infrastruktúrával, amellyel az adott szervezet nagy számú szervezeti egysége dolgozhat.

[1] Az Egyesült Államok Technológiai és Szabványügyi Nemzeti Intézete (NIST) által a felhő alapú számítástechnika fogalmára 2001. szeptemberében adott meghatározás http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- **Nyilvános felhő (public cloud).** A felhő infrastruktúra a nagyközönség vagy egy jelentős ipari csoport számára elérhető, és egy felhő alapú szolgáltatásokat értékesítő szervezet tulajdonában van. Az erőforrások kívülről hosztoltak, dinamikusan igénybe vehetők, és tipikusan strukturált árlista alapján kerülnek számlázásra. Példák: Microsoft Office 365, Amazon EC2, Microsoft Azure Platform, Salesforce.com, Google Apps.
- **Hibrid felhő (hybrid cloud).** A felhő infrastruktúra magán és nyilvános felhőkből tevődik össze, amelyeket általában külön-külön rögzített feltételek alapján bocsátanak rendelkezésre, de amelyek általában össze vannak kötve az adatok és alkalmazások hordozhatósága érdekében. Példa: nyilvános felhő, amely egyedi feladatterhelésekhez biztosít tehermentesítési kapacitást.

FELHŐ SZOLGÁLTATÁSI MODELLEK

A felhasználói igényektől függően a piacon számos felhő-szolgáltatási megoldás érhető el, amelyek három fő kategóriába, ún. ‘szolgáltatási modellbe’ sorolhatók. Ezek a modellek általában magán és nyilvános felhő megoldásokra is értelmezhetők:

- **Infrastruktúra mint szolgáltatás (‘IaaS’):** a felhőszolgáltató virtuális külső szervereket bocsát a felhasználók rendelkezésére különféle szolgáltatási mechanizmusok és szerződési feltételek szerint. Ez a modell ahhoz a helyzethez hasonlítható, amikor a felhasználók maguk telepítik fel az operációs rendszereket és az alkalmazásokat az új számítógépeikre, és saját maguk felelősek azért, hogy a teljes szoftver frissített és működtethető legyen. A tényleges különbség az, hogy a IaaS felhő esetén ezek az ‘új számítógépek’ fizikai értelemben nincsenek jelen, hanem csak ‘valahol a felhőben’ érhetők el ‘virtuális számítógép’ vagy ‘virtuális gép’ formájában, internet kapcsolat révén. A vevők a teljes szoftverek úgynevezett ‘image’-eit telepítik fel az ilyen virtuális szerverkörnyezetre. A szerződési feltételek rendszerint tartalmazzák a mért használattal arányos költségek elvét, és megengedik, hogy a végfelhasználó szükséglete szerint bővítse a rendelkezésére álló infrastruktúra használatát, általában önkiszolgáló portálokon keresztül. Például: Microsoft Azure Virtual Machines, Amazon EC2, Hosting.com, az IT által üzleti felhasználók számára nyújtott szolgáltatásként használatba vett / működtetett magán felhők.
- **Platform mint szolgáltatás (‘PaaS’):** a felhőszolgáltató alkalmazások hosztolására kínál megoldásokat. Ennek tartalma - az egyszerűség kedvéért – az, hogy a felhasználó virtuális számítógépet (‘virtuális gépet’) kap egy felhőben, amelyen egy operációs rendszer bizonyos típusa vagy verziója fut a kompatibilis alkalmazások feltelepítéséhez szükséges kiegészítő eszköz-könyvtárakkal együtt. Az összehasonlítás itt egy vállalati ERP szoftver telepítése egy távoli szerverre, amelyen Windows Server vagy Linux már telepítve van. A felhőszolgáltató kötelezettsége az operációs rendszer frissen tartása, és az összes szükséges hardver és hálózat működtetése. A PaaS-t széles körben használják új alkalmazások tesztelésére és bevezetésére anélkül, hogy szükség lenne helyi virtuális gépekre és a megfelelő szoftverekre. Ilyenre példák: Microsoft Azure Platform, Google App Engine, CloudFoundry.org.
- **Szoftver mint szolgáltatás (‘SaaS’)** olyan modell, amelyben egy alkalmazást az interneten keresztül nyújtanak, és azért a felhasználó a használat mértéke alapján fizet ellenértéket. SaaS esetében a felhasználó csak a kész alkalmazással dolgozik, azaz

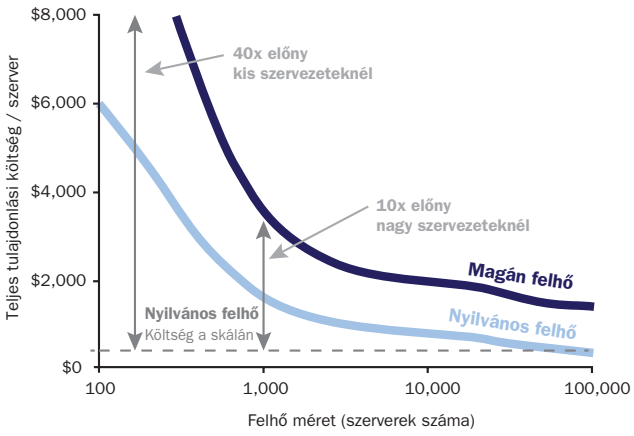
nem kell az alkalmazást, sem az ahhoz szükséges operációs rendszert vagy infrastruktúrát működtetnie. Ez a jelenleg leggyakrabban használt cloud computing szolgáltatásfajta. Példa erre: Microsoft Office 365, Salesforce.com, Hosted Exchange.

A LEGFONTOSABB ELŐNYÖK

Általános megközelítésben a cloud computing a következő előnyöket kínálja:

Lehetőség a globális piacra lépés akadályainak könnyebb leküzdésére a kis- és közepes vállalkozások („KKV") számára. A KKV-knak nem kell többé aggódniuk a saját fejlett szerver struktúráik működtetéséhez szükséges hardver, szoftver és rendszeradminisztráció igen magas bevezető költségei miatt. Gyorsan előfizethetnek egy, a felhőszolgáltatónál szükségleteik szerint rendelkezésre álló 'IT mint szolgáltatás'-ra. Így a KKV-k az elérhető legmodernebb, korábban csakis a legnagyobbak rendelkezésére álló informatikai infrastruktúra alkalmazása révén élénkíthetik üzleti aktivitásukat és innovatív képességeket, és ezzel a KKV-k a globális ellátási láncolataikban sokkal versenyképesebbé válhatnak.

A lekötött eszközök hányadának csökkenése a saját infokommunikációs infrastruktúra fenntartásának tőkeigényéhez képest. Számos hatékonysági tényező együttes hatása szól a cloud computing mellett: a szerverek nagyobb mérvű fizikai kihasználásától kezdve, a számítástechnikai erőforrásoknak a különféle ügyfelek közötti rugalmas újraosztásán át a rendszeradminisztráció magasabb mértékű automatizálásáig – mindezek hozzájárulnak az egyes ügyletekre vagy a működtetett szerverekre vetített fajlagos költségek csökkentéséhez. A szoftver eladók továbbá az alkalmazások szintjén rendelkezésre álló sokbérlős konstrukciók révén magasabb hatékonyságot érhetnek el, ami azt jelenti, hogy elég a forgalmazott szoftvert egyszer feltelepíteni a virtuális szerverre, és azt egyszerre elérhetővé lehet tenni több tucat vagy több száz egyidejűleg bekötött, egymástól virtuálisan elkülönített területeken működő felhő felhasználó (tipikusan KKV-k) számára. Az alábbi grafikon a Microsoft nyilvános felhők működtetésére vonatkozó költségbecslésén alapul, és azt fejezi ki, hogy a nagy méretű nyilvános felhő infrastruktúrában működtetett szerverekre eső teljes tulajdonlási költségek (total cost of ownership – TCO) 40-szer alacsonyabbak, összehasonlítva a KKV-k szerver infrastruktúrájának megfelelő értékével, vagy kb. 10-szer alacsonyabbak egy nagy felhő TCO hatékonyságával összehasonlítva:



Működtetett szerverekre vetített költség – kisvállalkozás, magán- és nyilvános felhők.[2]

[2] Microsoft Corp.: A felhő gazdaságtana az EU közszférában (2010), 17. oldal
http://www.microsoft.com/global/eu/RichMedia/eu_public_sector_cloud_economics_a4.pdf

Bárkiből lehet globális szoftver szállító. Szoftver start-upok vagy független, helyi szoftver értékesítők PaaS vagy SaaS megoldások értékesítése révén globális ellátók lehetnek – ezek a XXI. század ún. „mikro-globálisai". Bárki el tudja ugyanis adni a szoftvereit a különféle felhő alkalmazások szoftver piacainak egyikén akár SaaS-ként (mint pl. a Microsoft Azure Marketplace, a Salesforce AppExchange vagy a NEC Cloud Marketplace), akár felhasználási engedélyként a szintén a felhő alapú szolgáltatások közé tartozó mobil alkalmazások piacain (mint pl. a Windows Store, az Apple iOS App Store vagy a Google Play).

Mobilitás és rugalmas munkavégzés támogatása. Mivel mindenütt jelen lehetnek, és képesek az ügyfelek által használt mindenféle platform támogatására, a felhő alapú szolgáltatások ideális kiszolgálói minden PC-nek, táblagépnek, okostelefonnak és platformnak, és jó eséllyel a jövő testen viselt és beültetett készülékeinek. A szoftver mint szolgáltatás (SaaS) alkalmazásoknak, amelyekkel felhasználók ezreit láthatják el, nagyon gyorsaknak kell lenniük abban a tekintetben, hogy nagyszámú ügyfél-platformot szolgáljanak ki, amint azt az igen sokféle SaaS felhasználójuk elvárja. Elektronikus levelezési vagy naptár szolgáltatások vagy videokonferenciák felhő SaaS formájában történő igénybe vétele könnyebbé válik otthonról vagy távoli helyekről, ahol a 'hozd magaddal saját készülékedet' típusú stratégiát alkalmazzák. A vezető felhőszolgáltatók átlagos szolgáltatási biztonsága általában magasabb fokú, mint amelyet egy KKV meg tud fizetni, különösen, ha szünet nélküli, éjjel nappali, folyamatosan elérhető szolgáltatásra van igény.

Üzleti folytonosság és működési rugalmasság. A felhőszolgáltatók általában 99,9 %-os szolgáltatási szintet vállalnak a szerződéseikben. A Microsoft Office 365 szolgáltatásának átlagos elérhetősége 2013-ban 99.96% volt (amint azt az Office 365 Adatvédelmi Központ közzétette). Az ügyféladatokat általában[3] független merevlemezen tárolják az adatközpontokban, és sok felhőszolgáltató kínálja a mentett dokumentumok automatikus verziózását. A felhasználók választhatnak földrajzi redundanciát is, és szinkronizáltathatják az adataikat egy másik távoli adatközponttal, ami még nagyobb mértékű üzleti folytonosságot tesz lehetővé.

Kiberfenyegetés elleni védelem. Az elismert felhőszolgáltatók a 'szolgáltatás megtagadva' típusú támadások könnyű célpontjaivá válhatnak. Másfelől viszont a felhőszolgáltatók többnyire heti 168 órában tartanak fenn megfigyelést, amelyek kiber-támadás esetén képesek a felhasználók gyors figyelmeztetésére, és bőséges eszköztárral rendelkeznek, mint amilyen az ún. kapacitásbővítés (scaling-out capacity), a csomagszűrés (packet filtering) vagy a forgalom sebesség-szabályozása (traffic throttling) arra, hogy a felhő alapú szolgáltatások elérhetősége ne csökkenjen. A felhőszolgáltatók az elérhető leghatékonyabb vírus- és kártevőirtókkal és spamszűrőkkel rendelkeznek az e-mail, naptár- és a közös iratszerkesztési munka-szolgáltatás bemeneti pontjainál, amelyek a legújabb hálózati elemző technológiákat és az állandóan frissített kártevő programfelismerőket alkalmazzák.

[3] Office 365 Trust Center: http://trustoffice365.com/; Ld. „Office 365 availability" cím alatt

MŰSZAKI JELLEGŰ KIHÍVÁSOK ÉS LEHETSÉGES MEGOLDÁSOK

A jogi megfelelőségi problémákon kívül, amelyeket ez a kiadvány is tárgyal, vessünk egy pillantást a felhő alapú szolgáltatás legjelentősebb architekturális és működési kihívásaira:

A biztonság és a sokfelhasználós konstrukció közötti ellentmondás. A cloud computing hozadékai elsősorban a hatékony forrásegyesítésen és -megosztáson alapulnak, ami azt jelenti, hogy a felhőszolgáltatók céljai közt szerepel a sokfelhasználói elv magas szintű megvalósítása, tehát ideálisan az, hogy, az adott szoftver program használata nagyszámú felhasználó között kerüljön megosztásra. Ennél fogva fontos, hogy az alkalmazási környezet minden egyes felhasználó számára biztonságosan virtualizált legyen, az adataik legyenek egymástól elszigetelve, és lehetőség szerint biztonságos területek jöjjenek létre a közösen használt SaaS szolgáltatáson belül, mint amilyen az Office 365, hogy a felhasználó egyedi kódokat is futtatni tudjon

Integrált rendszeradminisztráció. Az előre látható jövőben csak kisszámú felhasználó fogja átvinni a teljes IT rendszerét felhőre. A legtöbb felhasználót ilyenféle kérdések foglalkoztatják: „nekem melyik felhőmodell a leginkább testhezálló?" és „milyen appokat kellene először felhőre átvinnünk?" Olyan rutinműveleteket, amelyeket a rendszergazdák visszatérőn végeznek, mint amilyen egy új felhasználói fiók létrehozása, vagy a virtuális gépük átméretezése, nagyfokú automatizálással kellene megoldani. Ideális esetben ugyanazokkal a rendszergazdai eszközökkel kellene kezelni a házon belüli és a felhőn lévő virtuális adatközpontokat is.

Biztonságos és egyszeri belépésű hozzáférés. Az online elérhető szolgáltatások bárhonnan való elérhetősége és a globális felhőhozzáférés lehetősége az internet révén felveti a kérdést, „hogyan biztosíthatjuk minden aktív dolgozónk számára a folytonos hozzáférést a felhő alapú szolgáltatásokhoz?" Ez olyan feladatokat tesz szükségessé, mint a felhőbe történő beléptetés erős kontrolljának kikényszerítése, a valós idejű dolgozói belépési jogosultság kezelése – különösen a szervezetbe történő be- és kilépések alkalmával -, és ideális esetben a valós egyszeri beléptetés megoldása a helyi és a felhő alapú szolgáltatásokba. Ez feltételezi a dolgozó státuszának dinamikus igazolását a belső nyilvántartásban úgy, hogy ne legyen észrevehető különbség aközött, hogy házon belüli vagy felhő alapú szolgáltatásba történik a belépés, történjen az akár a munkahelyi irodában, akár házon kívül végzett munka esetén.

Titkosítás és kód-management. A felhőszolgáltató tipikusan felel azért, hogy az ügyféladatok titkosítva legyenek az adattovábbítás ideje alatt (i) az ügyfél eszközéről a felhőbe és vissza, (ii) a biztonsági mentések adatközpontok közötti szinkronizálása során, és (iii) a felhőben fizikai merevlemezen történő adattárolás során. Más szervezeti biztonsági kontrollokkal együtt kellene elérni azt a biztonsági szintet, hogy a felhasználói adatokkal ne történhessen visszaélés. Mindamellett a felhőben érzékeny adatok tekintetében történő adatfeldolgozás szükségessé teheti a titkosítás egy további rétegét, amely teljesen kizárja a felhasználói adatokhoz nyílt formában történő hozzáférést addig, amíg azok a felhőbeli infrastruktúrában vannak. Ez újabb működési kihívásokat vet fel a titkosított ügyféladatoknak a felhőszolgáltató által való feldolgozása tekintetében, mint a keresés a dokumentumokban vagy az üzleti adatszerzés, amelyek vagy korlátozottak, vagy másfajta megközelítéseket igényelhetnek.

Szoftver verzió- és változásmanagement. A PaaS és a Saas szolgáltatások kiemelkedő előnyei közé tartozik, hogy „valaki más" (ti. a felhőszolgáltató) látja el a szoftver karbantartását, frissítését és javított verzióinak telepítését (a szoftver továbbfejlesztését). Ez azonban új kétségeket is támaszthat a felhasználó oldalán: vajon felkészültek vagyunk-e új verziók fogadására olyan ütemben, ahogyan azt a felhőszolgáltató előirányozza? Az ügyfeleink kellően felkészültek-e, be vannak-e tanítva erre? Nem merülnek-e fel integrációs problémák más rendszerekkel? Tanácsos lehet egyeztetni a felhőszolgáltatóval arról, hogy a felhasználónak van-e valamilyen beleszólási joga a szolgáltatás fejlesztéseknek a felhőből történő érkezési menetrendjébe.

KITEKINTÉS A FELHŐHASZNÁLAT MÉRTÉKÉNEK ALAKULÁSÁRA

Az International Data Corporation (IDC) 2013.[4] decemberétől lefolytatott kutatása szerint a felhő alapú szolgáltatások globálisan leggyorsabban fejlődő szegmense a SaaS lesz – a becsült növekedés mértéke csaknem ötszörös a szoftverpiac egészének növekedéséhez képest. 2016-ig csomagolt szoftverre, és alkalmazásokra elköltött minden 5 $-ból 1 $ felhasználása a SaaS modell alkalmazásával történik. 2016-ig a teljes üzleti szoftverbeszerzések hozzávetőleg 25%-a fog a szolgáltatásra kész szoftverekre esni, és a SaaS modell szerinti szállítások az elsődleges piacokon világszerte szoftverre elköltött összegek körülbelül 16,4%-át teszik ki, az alkalmazásokra költött összegeknek pedig 18,8%-át.

A cloud computing a jelenlegi „megatrendek" egyike – a mobilitás, a közösségi oldalak, a Business Intelligence / Big Data mellett. Az Ipsos MORI[5] egyik tanulmányában arra a következtetésre jutott, hogy az EMEA térségben (azaz Európában, a Közel-Keleten és Afrikában) a felhő alapú szolgáltatások népszerűsége a legnagyobb mértékben a KKV-k körében növekszik, ahol a vizsgált 6.800 társaság 53%-a már ma is legalább egyet használ a felsorolt felhő alapú szolgáltatások közül, mint az e-mail, adattárolás, dokumentumcsere, instant üzenetek, a VOIP, a Productivity Suite, videó konferencia és a processing power (a válaszadás szerinti gyakorisági sorrendben). 28%-uk úgy nyilatkozott, hogy a szervezetük a következő évben valószínűleg a ráfordításaik között az addiginál nagyobb arányban fog költeni felhő alapú megoldásokra. És ami a legfontosabb, közülük azoknak a 74%-a, akik már igénybe vesznek felhő alapú szolgáltatást, pozitívan nyilatkozott arról, hogy az IT megoldások mennyire segítik a munkájuk elvégzését; akik viszont nem használnak felhő alapú szolgáltatásokat, azok körében ez az arány csak 61% volt. A felhőt használó KKV-k üzleti kilátásaikat illetően nagyobb mértékben voltak bizakodók (33%), mint azok, amelyek nem használnak felhőt (26%), és akik már használják a felhőt, azok gyakrabban tervezték új termékek vagy szolgáltatások piaci indítását, újabb piacokon való megjelenést, és befektetéseket a hatékonyság vagy a termelékenység növelése érdekében.

Általánosságban a felhőben rejlő és az üzleti vezetők által felismert legnagyobb lehetőségek (i) az IT hatékonyság – számítástechnikai erőforrások gyors szállítása elfogadható árakon, (ii) IT mozgékonyság – könnyen használható, állandó és használattal arányosan fizetendő szolgáltatásokkal, és (iii) az üzleti innováció – a felhő révén a vevőkkel kapcsolatos lehetőségekre gyorsabb válaszok adhatók, és az üzleti teljesítést, annak optimalizálását ténylegesen előmozdítja a felhő. A felhő alapú szolgáltatások először a készen vásárolt és a munkahelyen telepített szoftvereket váltják ki (pl. az e-mailt, közös munkát, naptári előjegyzést, telefon- és videokonferenciát), az adatmentést és archiválást, és újabb fejleményként már olyan üzleti folyamatokat, mint az ügyfélkapcsolat-kezelés (CRM), a bérszámfejtés, beszerzés és más webes alkalmazások.

[4] IDC Market Analysis Perspective: SaaS and felhő szoftver világszerte, 2013 (IDC #245047) http://www.idc.com/getdoc.jsp?containerId=245047

[5] Ipsos MORI: Kisvállalkozások és a felhő alapú számítástechnika EMEA régiós tanulmány (2013) http://download.microsoft.com/download/3/5/2/35261139-417E-43B1-84A6-663646881E11/Microsoft%20EMEA%20SMB%20Cloud%20Survey%202013.pdf

CLOUD COMPUTING ÉS **ADATVÉDELEM**

Mgr. Jana Pattynová, LL.M., *partner, PIERSTONE*
Mgr. Lenka Suchánková, LL.M., *partner, PIERSTONE*

A cloud computing először marketing-kifejezés volt, majd pedig egy növekvő mértékben közhasználatúvá váló, a számítástechnikai felhasználók egyre növekvő tömegét napi szinten (akár az érintettek tudta nélkül) kiszolgáló eszköz elnevezése lett. Technikai szempontból és dióhéjban összefoglalva, a cloud computing olyan szolgáltatásként jellemezhető, amely könnyű hozzáférést tesz lehetővé a felhasználói számára az interneten keresztül konfigurálható olyan IT eszközökhöz, mint a hálózatok, szerverek, adattárolók vagy alkalmazások és programok. Az adatok és programok a felhasználó számítógépe helyett külső, a felhasználótól gyakran több ezer kilométer távolságra levő szervereken tárolhatók. Ebben a szövegösszefüggésben a távoli szerver megjelölésére általában a felhő kifejezést használják, a felhő alapú számítástechnika kifejezés innen ered.

Európai jogi szempontból a cloud computing, összhangban az Európai Parlament és a Tanács 2001/29/EK (2001. május 22.) irányelvével a szerzői és a szomszédos jogok bizonyos aspektusainak az információs társadalommal történő összehangolásáról, fogalmilag szoftver helyett inkább szolgáltatásnak tekinthető. Ennek a felfogásnak egy fontos következménye az, hogy összehasonlítva hagyományosabb licenc modellekkel, a jogok kimerítésének elve nem lenne alkalmazható az infokommunikációs szolgáltatások felhő alapon történő nyújtására. Az EU joga sem jogi definíciót, sem egy teljes értékű jogi keretet nem ad a cloud computing-ra, mégis nyilvánvaló, hogy, legalábbis az EU szintjén, a legnagyobb jogi figyelmet a cloud computing-gal kapcsolatban az adatvédelem és –biztonság területére kell fordítani, közelebbről a személyes adatok védelmére. Ez a cikk az EU személyes adatok védelmét szolgáló általános jogszabályainak szemszögéből kíván rálátást nyújtani a cloud computing egyes aspektusaira, kis kitérővel a szektorfüggő specifikus szabályozásra.

SZEMÉLYES ADATOK ÉS A ’FELHŐ’ – KIK A KULCSSZEREPLŐK?

Mára általánosan elfogadott, hogy a felhő alapú szolgáltatások, legyen szó akár az Saas, a PaaS vagy a IaaS modellről, valamilyen módon és mértékben magukban foglalják személyes adatok feldolgozását. A különböző cloud computing szolgáltatási struktúrákban különféle szereplők működnek közre, és az EU személyes adatvédelmi szabályozásának szempontjából a felhőszolgáltatók játsszák az ‘adatfeldolgozó’, míg az adatkezelés / adatfeldolgozás végső célját meghatározó felhasználóik döntenek az adatkezelési tevékenység egy részének vagy egészének külső szereplőre történő kiszervezéséről vagy delegálásáról, és a legtöbb esetben ‘adatkezelő’-nek minősülnek. Ez a szabály azonban nem feltétlenül érvényesül, és a kulcsszereplők szerepének minősítése nagyban függ az adott eset konkrét körülményeitől. Például, ha egy felhőszolgáltató a rábízott személyes adatokat saját érdekkörében kezeli, akkor együttes adatkezelőnek minősülhet, sőt akár a saját jogán adatkezelőnek is.

A fenti két szereplő közötti felelősséget meghatározó szabályok szerint, ahogyan azt a 29. cikk szerint

létrehozott Adatvédelmi Munkacsoport 05/2012. számú, a felhő alapú számítástechnikáról kibocsátott, 2012. július 1-jén keltezett véleményében (a „Felhő Vélemény")kifejtette, elsősorban a személyes adat kezelője – azaz a felhő alapú szolgáltatás igénybevevője – felelős azért, hogy mindenkor garantálja a felhőszolgáltatóra általa bízott személyes adatok szigorú elvárásoknak megfelelő biztonságát. Ennek megfelelően a felhőszolgáltatás igénybevevője köteles lefolytatni a felhőszolgáltatáshoz kapcsolódó lehetséges kockázatok érdemi elemzését, és gondoskodni a megfelelő technikai és biztonsági intézkedésekről, valamint hatékony szerződési biztosítékokról (beleértve azokat is, amelyek a határokon átnyúló személyes adatmozgások jogszerűségét hivatottak biztosítani), mégpedig azt megelőzően, hogy egy harmadik személy által nyújtott, felhő alapú szolgáltatást használatba venne.

ADATFELDOLGOZÁSI MEGÁLLAPODÁS

A felhőben végzett adatfeldolgozás egyik pillére az írásbeli (vagy „egy azzal egyenértékű más formában megkötött") megállapodás a személyes adatok feldolgozásáról (az „adatfeldolgozási megállapodás"). Adatfeldolgozási megállapodást kell kötni az adatkezelő és az adatfeldolgozó között, még mielőtt a felhőben bármiféle adatfeldolgozási műveletre sor kerülne. A legkevesebb, amit az ilyen megállapodásnak tartalmaznia kell, az a rendelkezés, hogy az adatfeldolgozó az adatkezelő utasításainak megfelelően köteles eljárni, valamint rendelkeznie kell azokról a technikai és szervezési intézkedésekkel kapcsolatos garanciákról, amelyeket az adatfeldolgozó köteles nyújtani a személyes adatoknak véletlen vagy jogellenes megsemmisítése, valamint a véletlenül bekövetkező adatvesztés, változás, illetéktelen adattovábbítás vagy hozzáférés, és a feldolgozás minden más, jogellenes módja elleni védelme érdekében. Az EU tagállamainak lehetőségük van, és rendszerint élnek is ezzel, hogy az adatfeldolgozási megállapodásban szabályozandó további követelményeket határozzanak meg, mint amilyen a feldolgozandó személyes adatok közelebbi meghatározása és a feldolgozás terjedelme, a feldolgozási cél és időszak, vagy a felelősségek megosztása a szerződő felek között.

TÖBB ALANY A FELDOLGOZÓI OLDALON

A felhő alapú szolgáltatások gyakran járnak azzal, hogy az adatfeldolgozásba szerződő félként mint feldolgozó vagy al-feldolgozó számos személy kapcsolódik be az eredeti feldolgozó oldalán. Általánosságban az alfeldolgozói közreműködés megengedett, feltéve, hogy a feldolgozó tájékoztatja erről a felhő felhasználót, feltárva előtte az alfeldolgozásba adott szolgáltatási típus részleteit, a meglévő és lehetséges alfeldolgozók jellemzőit, és garanciákat vállal arra, hogy a teljesítésébe bevont személyek vállalják az EU Adatvédelmi Irányelvének érvényesülését szolgáló jogszabályok betartását, illetve azt, hogy az adatfeldolgozót az adatkezelővel kötött megállapodás szerint terhelő kötelezettségek megfelelően megjelennek az alfeldolgozókkal ugyancsak megfelelő módon és tartalommal kötött vagy megkötendő szerződésekben is.

HA A FELHŐSZOLGÁLTATÓ KÜLFÖLDÖN MŰKÖDIK

A cloud computing szolgáltatás globális jellegéből következően azok az adatközpontok, ahol a felhasználók adatait tartják, gyakran kívül vannak annak az országnak a határain, ahol a felhasználó működik. Ennél fogva a felhő alapú szolgáltatások használata gyakran jár személyes adatok határokon átívelő mozgásával, ami viszont megköveteli, hogy a felek fokozott figyelmet szenteljenek a megfelelő adattovábbítási feltételrendszernek.

A személyes adatoknak határokon túlra való továbbításáról szóló szabályok különböznek a szerint, hogy a személyes adatokat melyik országba küldik. A személyes adatoknak az EU és az EGT határain belül történő továbbítása nem korlátozható, ezért azok mindenféle megszorítás nélkül, szabadon áramoltathatók (feltéve, hogy az adatfeldolgozásra vonatkozó egyéb jogszabályokat betartják, például azt, amely a megfelelő technikai és szervezési biztonsági intézkedésekről rendelkező adatfeldolgozási megállapodás meglétét írja elő). Ugyanazon szabályok vonatkoznak az adattovábbításra olyan országokba, amelyek tagjai az egyének személyes adatok automatikus feldolgozása során történő védelméről szóló egyezménynek (Európa Tanács, ETS 108, 1981). Hasonlóképpen megengedett a személyes adatok korlátozás nélküli továbbítása azokba az országokba, amelyeket az Európai Bizottság kifejezett döntésével „biztonságosnak" minősített (mint például Argentínát, Izraelt vagy Új-Zélandot).

Ha viszont olyan országokba kívánnak személyes adatokat továbbítani, amelyek nem rendelkeznek a személyes adatok megfelelő szintű védelmével, az esettől függően külön biztonsági intézkedéseket tesz szükségessé, mint amilyen az EU-US Biztonságos Kikötő Keretszabályok, az EU Általános Szerződési Feltételek vagy a Kötelező Erejű Vállalati Szabályok („BCR"). Az Európai Bizottságnak az Európai Parlament és a Bizottság 95/46/EK számú irányelve alapján 2000. július 6-án hozott az Egyesült Államok Kereskedelmi Minisztériuma által kiadott 'Biztonságos Kikötő' adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos, gyakran felvetődő kérdésekről szóló határozatát (az „EU-US Biztonságos Kikötő Keretszabályok"), amely arra az esetre vonatkozik, ha személyes adatokat egy, az Egyesült Államokban lévő, igazoltan „Biztonságos Kikötőként" elismert entitáshoz továbbítanak, újabban éles, és növekvő mértékű kritika érte az EU intézmények és egyes vezető személyiségek - különösen Viviane Reding, az Európai Bizottság igazságügyi, alapjogi és állampolgársági biztosa - részéről. Mivel gyűlnek a felfüggesztését sürgető indítványok, és az euro-atlanti szerződéses rendszer 2014. nyarára kitűzött felülvizsgálata is napirenden van, az olyan európai felhő felhasználóknak, akik a személyes adatoknak az Egyesült Államokba való továbbítása tekintetében az EU-US Biztonságos Kikötő Keretszabályokra támaszkodnak, tanácsos szoros figyelemmel kísérniük a fejleményeket, mert a jövőben kénytelenek lehetnek alternatívákat keresni, amelyek az Atlanti óceán túloldalára történő adattovábbítások jogszerűségét garantálni tudják.

Jelenleg a személyes adatoknak határokon túlra, olyan országokba történő továbbítására, amelyek nem biztosítanak az EU személyes adatvédelmi szabályainak megfelelő szintű védelmet, a fő alternatívát kétség kívül az EU Általános Szerződési Feltételek jelentik.

A 29. cikk szerint létrehozott Adatvédelmi Munkacsoport véleménye az, hogy az EU-US Biztonságos Kikötő Keretszabályok[1] alapján maga az érintett entitás által kiállított igazolás önmagában, a felhő környezetben is hatékonyan kikényszerített személyes adatvédelmi elvek érvényesülésének hiányában, nem tekinthető megfelelő védelemnek; ezzel szemben az EU Általános Szerződési Feltételek mint a személyes adatokat harmadik országba továbbító felhasználók számára hatékony védelmet kínáló feltételek általánosan elfogadottak. Ezért a 29. cikk szerint létrehozott Adatvédelmi Munkacsoport az európai adatexportőröket arra bátorítja, hogy ezt a jogi eszközt használják (a BCR mellett, amelynek használata viszont egy-egy vállalatcsoporton belüli adatmozgásokra korlátozódik, és mint ilyen, a felhőszolgáltatók szempontjából csak kis mértékben releváns). Bár az EU Általános Szerződési Feltételeket számos EU tagállamban úgy ítélik meg, mint amelyek személyes adatok számára megfelelő biztonságot jelentenek, és változatlan formában történő használatuk nem igényel hatósági jóváhagyásokat sem, néhány uniós tagállam jogszabályai mégis előírnak az Adatvédelmi Hatóságtól valamilyen előzetes jóváhagyást, illetve a hatóságnak való előzetes bejelentést.

A CLOUD COMPUTING MEGÁLLAPODÁSOK ELVI ALAPJAI

A Felhő Vélemény hangsúlyozza, hogy a személyes adatok felhőben történő feldolgozásának jogszerűsége nagy mértékben bizonyos alapelvek megtartásán múlik, amelyek az EU adatvédelmi jogának alappillérei, nevezetesen az adatgazda számára való átláthatóság, az arányos és célhoz kötött adatkezelés elve, valamint az adatvédelmet és adatbiztonságot biztosító megfelelő szerződési biztosítékok megvalósítása. Ezeknek az elveknek a tartalma az alábbiak szerint foglalható össze:

- **Átláthatóság.** A felhő felhasználóját mindenkor tájékoztatni kell a személyes adatok védelmét érintő minden lényeges körülményről, különösen bármilyen alvállalkozó bevonásáról a feldolgozásba, a helyekről, ahol az adatok tárolása vagy feldolgozása történik, valamint a szolgáltató technikai és szervezési intézkedéseiről.

- **Arányos és célhoz kötött adatkezelés.** Korlátozó szerződési kikötések (mint amilyen annak a kifejezett megtiltása, hogy a szolgáltató a felhasználó adatait reklámcélra felhasználja), és annak a szerződésben történő rendezése, hogy az adatok feldolgozási céljának a megszűnése, és különösen a szerződés megszűnése után megtörténjen az adatok törlése, be kell hogy kerüljenek a cloud computing szerződésbe. Különösen javasolt arról szóló kifejezett rendelkezés szerepeltetése a megállapodásban, hogy az adatok tulajdonjoga nem száll át a felhőszolgáltatóra.

- **Általános szerződési biztosítékok.** Egy cloud com-

[1] Az Európai Bizottságnak a 95/46/EK irányelv alapján hozott, 2010. február 5-én kelt döntése a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről.

puting szerződésnek meg kell határoznia a felhőszolgáltató által megvalósítandó biztonsági intézkedéseket, valamint a felhő felhasználója által a szolgáltatónak adható utasítások terjedelmének és módozatainak a részleteit, beleértve a szolgáltatási szinteket és a szolgáltatási szintek be nem tartása esetére rendelt szankciókat (amelyek általában a szolgáltatási szintek megsértéséhez kapcsolódó kötbérek, vagy jóváírások és díjkedvezmények szerinti modellben kerülnek meghatározásra).

- **Az adatokhoz való hozzáféréshez kapcsolódó szerződési biztosítékok.** Kizárólag kifejezett jogosultsággal rendelkező és titoktartásra kötelezett személyek részre adható hozzáférés a felhőben tárolt adatokhoz.

Tekintetbe véve a fentiekben említett kritériumokat és a felhő felhasználók adatkezelőként viselt felelősségét, a lehetséges felhő felhasználók számára kiemelkedően fontos a felhőszolgáltató körültekintő megválasztása. Egy elismert felhőszolgáltató kiválasztása segít abban, hogy, egyebek mellett, magas szinten valósuljon meg a felhőben tárolt személyes adatok biztonsága, és minimalizálható legyen az adatvédelmi hatóságok által kiszabott esetleges bírságoknak való kitettség. Egy meghatározott biztonsági szint és a megfelelő adat-management meglétének igazolására a felhasználók egyre gyakrabban várják el felhőszolgáltatóiktól különféle szintű és formájú, széles körben elfogadott tanúsítványok bemutatását, mint amilyenek az ISO 27001 és 27002 számú általános szabványoknak megfelelést igazoló tanúsítványok, amelyek le is írják a fizikai és online biztonság fenntartása érdekében szükséges intézkedéseket, valamint a jogsértésekkel szemben teendő válaszlépéseket.

EGYÉB ADATOK A FELHŐBEN

A személyes adatokon kívül a felhő szolgáltatások szokásos használója tömegesen tárol a felhőben nem személyes adatokat is. Mivel ezek gyakran üzletileg érzékeny adatok, nem elhanyagolható ezeknek a védelme sem. Nem szokatlan, ha egy felhő felhasználó megköveteli, és a szolgáltató vállalja is, hogy ugyanazt a biztonsági szintet biztosítják ezeknek a nem személyes, de tulajdonként védeni kívánt adatoknak, mint amely védelmi szintet a személyes adatok élveznek.

Az ördög, persze, a részletekben bújik meg, és a felhőszerződések gyakran tartalmaznak olyan rendelkezéseket, amelyek első pillantásra viszonylag ártalmatlannak látszanak, de valójában széles körű jogosítványokat adhatnak a felhőszolgáltatónak azokon túl, amelyeket a tisztán adatfeldolgozási tevékenység szigorúan megkövetelne: ilyen az adatkezelő adatai ellenőrizetlen használatának lehetővé tétele (akár haszonszerzési célból) a feldolgozó számára. Még standard felhő szolgáltatási szerződésekben is előfordulhatnak rendkívül agresszív kikötések, amelyek adatbányászatot tesznek lehetővé, gyakran felhasználóbarátnak álcázott szövegezésben, mint amely például „célzott és testre szabott tartalmat” ígér.

A közelmúltnak a Snowden-ügy körüli fejleményei rávilágítottak arra az ellentmondásos kérdésre, hogy az állami hatóságok hozzáférhetnek-e a felhőben tárolt adatokhoz. Az iparág reagált ezekre a felismerésekre, és néhány felhőszolgáltató indítványt is tett a hatósági megfigyelési gyakorlat reformjára, világosabb szabályokat és jobb átláthatóságot igényelve. A felhőszolgáltatók közül néhányan közzé is tesznek információt – megengedett mértékben – az ügyfelek

adataival kapcsolatos megkeresések mennyiségéről, típusáról és annak hatásáról;[2] forráskódokat osztanak meg annak érdekében, hogy a vásárlók megbizonyosodhassanak: nincsenek „hátsó ajtók", amelyeken keresztül az állami hatóságok hozzáférhetnének az adataikhoz, valamint a felhőszolgáltatók egyéb intézkedések mellett fokozzák a titkosítást. A maximális biztonság garantálása érdekében, ti. hogy a felhasználó adatait nem kezelik önkényesen és a tudta nélkül, helyénvaló részletes szabályozás formájában megállapodni a felhőszolgáltatóval az ilyen adatigénylésekről, és a felhőszolgáltatót terhelő olyan kötelezettséget beépíteni, hogy a felhőszolgáltató köteles legyen meggyőződni adott esetben arról, hogy a szóban forgó hatóság valóban jogosult-e az adott hatósági jogosítványt gyakorolni.

FELHŐ SPECIÁLIS ÁGAZATOKBAN

Ami a szektor-specifikus szabályozást illeti, azt általánosságban le lehet szögezni, hogy nincs olyan szektor, ahol a felhő alapú szolgáltatás használata eleve ellentmondásban lenne a jogi szabályozással. Bizonyos ágazatokban, mint a bankszektorban, egészségügyben vagy a közszférában speciális kötelezettségek vagy szabályok alkalmazandók, amelyekre felhőszolgáltatások igénybevétele során figyelemmel kell lenni. A szektorspecifikus szabályozás tipikusan olyan témák körül forog, mint a kockázatértékelés, a felhőszerződésre irányadó speciális követelmények (kiváltképpen a biztonság körül), a bizonytalansági tényezők felmérése és kilépési lehetőség a szerződésből, a szektorbeli felhő felhasználó vagy a szabályozó hatóság kifejezett felhatalmazása arra, hogy megvizsgálja, illetve auditálja a kiszervezett adatok feldolgozásának mozzanatait, rendszerét és eszközeit.

Megszokottá válik, hogy a nagy nemzetközi felhőszolgáltatók tanúsítványt készítenek az adatfeldolgozó műveleteik és eszközeik tekintetében; ebben a tekintetben az új ISO 27018 szabvány valószínűleg az iparág új standardja lehet. Ha egy felhő felhasználó kisebb felhőszolgáltatóval szerződik, több időt és figyelmet kell fordítania a biztonsági szint alapos vizsgálatára annak érdekében, hogy a számára is megnyugtató, megfelelő biztonsági követelmények érvényesülni fognak.

A piacon elérhető olyan felhő alapú termékek, amelyeket elismert, jelentős felhőszolgáltatók kínálnak, egyre inkább megfelelnek „a beépített adatvédelem" (privacy by design) követelményének, azaz eleve olyan módon vannak megalkotva, hogy összhangban legyenek a személyes adatvédelemről szóló jogi szabályozással. Az egyes szerződési konstrukciók egymástól lényegesen eltérőek lehetnek attól függően, hogy hová történik a személyes adatok továbbítása, és mi a felhőszolgáltatók jogosítványainak a terjedelme a felhasználók felhőben tárolt adatai tekintetében. A szerződési feltételek, és ahol alkalmazandók, a szektor-specifikus követelmények alapos áttekintése és értékelése egy körültekintő felhő felhasználó számára elengedhetetlen követelmény. Végül, de nem utolsó sorban, a felhő felhasználóknak szem előtt kell tartaniuk azt is, hogy az információs technológiai biztonság a felhő alapú szolgáltatások kontextusában jelentősen eltér a hagyományos infokommunikációs technológiai szolgáltatások klasszikus modelljeitől, és a különbségeknek meg kell jelenniük a felhőszolgáltatók és a felhő felhasználók közötti megállapodások szerződési feltételeiben.

[2] Ld. például http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ or http://www.google.com/transparencyreport/removals/government/

ÁLTALÁNOS KÖVETELMÉNYEK AZ EU ADATVÉDELMI JOGA

A JOGI TANÁCSADÓ ELÉRHETŐSÉGI ADATAI:

Ügyvéd: Lenka Suchánková
Ügyvédi Iroda: PIERSTONE s.r.o., advokátní kancelář
Na Příkopě 9
110 00 Prága 1
Cseh Köztársaság
Website: www.pierstone.com
E-mail: enka.suchankova@pierstone.com

Az alábbi táblázat célja, hogy megjelölje a legfontosabb irányadó adatvédelmi témákat, amelyeket a felhőszolgáltató kiválasztása előtt a felhasználónak tudnia és értékelnie kell. Nem tartalmazza azonban az európai adatvédelmi követelmények vagy más alkalmazandó jogszabályok kimerítő ismertetését.

Az alább következő válaszok alapja az EU Adatvédelmi Irányelve és a Felhő Vélemény, valamint azok a források, amelyeket hivatkozásként kifejezetten megjelöltek. Ahol az EU Adatvédelmi Rendeletének Tervezete jelentős változtatást hozhat, ott arra kifejezett figyelemfelhívás történik.

BEVEZETÉS

1

Mi a „személyes adat” definíciója? Személyes adatnak tekintendő-e a titkosított adat, ha a titkosítási kód nincs a felhőszolgáltató birtokában?

A személyes adat meghatározása szerint „az azonosított vagy azonosítható természetes személyre („érintettre”) vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén”.[1]

[1] Ld. a személyes adat fogalom-meghatározását az EU 95/46/EC irányelve 2. cikk a) pontjában.

Jelenleg nincs EU szintű kötelező érvényű döntés vagy iránymutatás abban a tekintetben, hogy mikor tekinthetők a kódolt adatok biztosan a személyes adatok védelmi körén[2] kívül eső anonimizált adatoknak. Az EU Adatvédelmi Rendeletének Tervezete várhatóan kifejezetten szabályozni fogja az anonimizált adatok használatát. Az EU Adatvédelmi Rendeletének jelenlegi Tervezete azt az álláspontot rögzíti, hogy az adatvédelem elveit nem kellene alkalmazni az olyan módon anonimmá tett adatokra, amelyek eredményeként az érintett már nem azonosítható. Így helyénvaló lehet az a következtetés, hogy amikor a felhőszolgáltatóknak nincs hozzáférésük a dekódoláshoz szükséges kulcshoz, sem más, 'ésszerű valószínűséggel' dekódolásra használható módszerhez, akkor az általuk kezelt kódolt adatok ne minősüljenek személyes adatoknak; az ilyen adatok inkább anonimizáltnak tekintendők.

2

Melyek a fő szempontjai annak, hogy az EU adatvédelmi jogszabályainak alkalmazhatósága megállapítható legyen?

Az EU adatvédelmi jogszabályait kell alkalmazni minden adatkezelőre (felhő felhasználók), amelynek egy vagy több telephelye van az EU-n belül, valamint minden adatkezelőre, amely kívül van ugyan az EU területén, de az EU-n belüli eszközt használ a személyes adatok feldolgozására, kivéve, ha az ilyen berendezést kizárólag az EU területén átmenő adatforgalom céljára használják.

[2] Például a Felhő vélemény azt az álláspontot képviseli, hogy bár a kódolás, ha helyesen végzik el, jelentősen hozzájárulhat a személyes adatok titokban tartásához, az nem teszi a személyes adatot visszafordíthatatlanul anonimmá. Másrészt a WP 29 4/2007 számú véleménye a személyes adatok elvéről azt állítja, hogy az egyirányú kriptográfia általában anonimmá teszi az adatokat, azaz nem-személyessé: „A személyazonosság elfedése olyan módon is lehetséges, hogy a visszaazonosítás lehetetlenné váljon, azaz egyirányú kódolás útján, amely általában anonimizált adatokat hoz létre". További észrevételek az eljárás hatékonyságáról azt látszanak támogatni, hogy a minősítés mikéntjének kulcstényezője, ti. hogy a kódolt adatokat anonim adatoknak lehet-e tekinteni, az egyirányú folyamat visszafordíthatósága vagy visszafordíthatatlansága.

FELHASZNÁLÓ / FELHŐSZOLGÁLTATÓ / ALADATFELDOLGOZÓ – FELADATOK ÉS FELELŐSSÉGI KÖRÖK

3

Általánosságban ki az adatkezelő, és ki az adatfeldolgozó egy felhő alapú szolgáltatás során? Írja le a fő kötelezettségeiket.

Az adatkezelő tipikusan a felhő felhasználó: ő határozza meg az adatkezelés végső célját, és dönt arról, hogy a feldolgozási tevékenység egy részét vagy egészét delegálja-e külső szervezetre (a felhőszolgáltatóra).

A felhőszolgáltató általában adatfeldolgozónak tekintendő, aki a személyes adatokat a felhasználó érdekében dolgozza fel (adatfeldolgozó). Előfordulhat ugyanakkor olyan helyzet, amikor a felhőszolgáltató vagy együttes adatkezelőnek, vagy a saját jogán adatkezelőnek minősülhet, pl. amikor a felhőszolgáltató saját céljaira kezel személyes adatokat.

A felhő felhasználó teljes mértékben felelős marad az adatfeldolgozás jogszerűségéért. A felhőszolgáltatók kötelesek a személyes adatok bizalmas kezelésére, és csak az adatkezelő (felhasználó) utasítására végezhetnek adatfeldolgozást, kivéve, ha azokat jogszabály rendelkezése alapján kötelesek bármely más célra feldolgozni. A felhőszolgáltatók mint adatfeldolgozók kötelesek továbbá technikai és szervezési biztonsági intézkedéseket foganatosítani (ld. az 5. kérdést), valamint támogatni és segíteni az adatkezelőt az érintett személy jogainak érvényesítésével kapcsolatban.

4

Szükséges-e adatfeldolgozási megállapodás a felhőszolgáltató és a felhasználója között? Írja le annak minimális tartalmát.

Igen. A megállapodásnak rendelkeznie kell különösen arról, hogy (i) az adatfeldolgozó csakis az adatkezelő utasításai szerint járhat el, és (ii) az adatkezelőkre az EU jogszabályai szerint irányadó jogi kötelezettségek irányadók az adatfeldolgozóra is. Ezek a kötelezettségek magukban foglalják megfelelő technikai és szervezési intézkedések foganatosítását a személyes adatoknak véletlen vagy jogellenes megsemmisítése, valamint a véletlenül bekövetkező adatvesztés, változás, illetéktelen adattovábbítás vagy hozzáférés elleni védelme érdekében (ld. az 5. kérdést).

5

Foglalja össze a technikai és szervezési intézkedéseket, amelyeket a felhőszolgáltató köteles betartani.

A felhőszolgáltató köteles különösen

(i) Ésszerű óvintézkedéseket bevezetni a szolgáltatás megszakadás kockázatának kezelésére, mint amilyenek az internet hálózati adatmentési linkek, a redundáns tárolás és a hatékony biztonsági mentési mechanizmusok;

(ii) Biztosítani a személyes adatok épségét behatolásjelzés / megelőző rendszerek alkalmazásával;

(iii) Kódolni a személyes adatokat „in transit" idején, és, ahol elérhető, az adatok „nyugalmi helyzetében"[3] is. A titkosítást a felhőszolgáltató és a felhő felhasználó, valamint az adatközpontok közötti kommunikáció idején is alkalmazni kell;

(iv) Megfelelően kézben tartani a személyes adatokhoz hozzáféréshez való jogot, illetve szerepeket, és ezek eljárásait rendszeres időszakonként felülvizsgálni;

(v) Garantálni az adatok hordozhatóságát;

(vi) Olyan további tevékenységeket is elvégezni, mint az összes adatfeldolgozási művelet azonosítása, válaszadás az adatokkal kapcsolatos hozzáférési kérésekre, a források elosztása, beleértve az adatvédelmi követelményeknek való megfelelést biztosító adatvédelmi felelősök kijelölését, és ezeknek az intézkedéseknek a dokumentálása.

A felhőszolgáltatónak lehetősége van arra, hogy független harmadik személy auditálása vagy igazolása útján igazolja az adatvédelmi szabványoknak való megfelelését, valamint a megfelelő és hatékony biztonsági intézkedések bevezetését, azzal, hogy az auditnak teljesen átláthatónak kell lennie.

6

Megengedett-e, hogy a felhőszolgáltató alfeldolgozót vegyen igénybe?

Igen, általánosságban megengedett, hogy a felhőszolgáltatók alvállalkozásba adják az adatfeldolgozási szolgáltatást alfeldolgozóknak, amihez szükséges viszont az adatkezelő előzetes hozzájárulása. Az ilyen hozzájárulás megadható a szolgáltatás megkezdésekor, de az adatfeldolgozó egyértelmű kötelessége informálni az adatkezelőt minden tervezett változtatásról, így a teljesítésbe további alfeldolgozó bevonásáról vagy más al-feldolgozó lecseréléséről. Az adatkezelő számára fenn kell tartani a jogot a jelzett változtatás miatti tiltakozásra vagy a szerződés felmondására.

[3] A Felhő Vélemény tartalmazza azt az álláspontot is, hogy bizonyos esetekben (pl. IaaS tárolási szolgáltatáskor) egy felhő ügyfél elfogadhatja a felhőszolgáltató által felajánlott titkosítási megoldást, de választhatja azt is, hogy a felhőre küldés előtt kódolja a személyes adatokat. A Felhő Vélemény szóhasználata („ahol elérhető") arra utal, hogy a Felhő Vélemény elismeri, miszerint a titkosítás nem minden esetben megvalósítható megoldás.

NEMZETKÖZI ADATTOVÁBBÍTÁSOK

7

Melyek a személyes adatok EGT-n belül történő továbbításának követelményei?

Nincsenek speciális követelményei a személyes adatok EGT-n belüli továbbításának.

8

Melyek a személyes adatok EGT-n kívüli továbbításának követelményei?

Személyes adatok csak akkor továbbíthatók harmadik országokba, ha azok a harmadik országok biztosítják az adatvédelem megfelelő szintjét. Ha a védelem megfelelő szintjét egy konkrét harmadik országban a Bizottság egy döntésével az illető ország tekintetében nem erősítette meg, akkor az adatkezelő kizárólag az alábbi továbbítási mechanizmusokra támaszkodhat:

(i) EU-US Biztonságos Kikötő Keretszabályok: USA-beli szervezetekhez személyes adat továbbítása az EU joga szerint akkor jogszerű, ha az USA-beli szervezet kötelezően betartja a Biztonságos Kikötő Keretszabályokat, miáltal a fogadó szervezeteket úgy kell tekinteni, mint amelyek biztosítják a továbbított személyes adatok védelmének megfelelő szintjét. A Felhő Vélemény szerint azonban pusztán az, ha a fogadó szervezet saját maga igazolja, hogy biztonságos kikötőnek minősül, önmagában, erős és határozott jogérvényesítő erő hiányában, felhő környezetben nem feltétlenül felel meg az elvárásoknak. Ezért a felhőszolgáltatók további olyan biztosítékokat is kínálnak, mint az EU Általános Szerződési Feltételek.

(ii) EU Általános Szerződési Feltételek: Az adattovábbításban résztvevő felek (az EU-beli adatkezelő és adatexportőr, valamint harmadik országbeli adatfeldolgozó és adatimportőr) EU Általános Szerződési Feltételeket köthetnek, amelyek úgy tekintendők, mint amelyek az EU Adatvédelmi Irányelvének megfelelő biztonságot ajánlanak a személyes adatok védelme tekintetében.

(iii) Kötelező Erejű Vállalati Szabályok („BCR”): A BCR olyan társaságok számára tartalmaz magatartási szabályokat, amelyek a vállalatcsoportjukon belül továbbítanak adatokat, és ezek felhasználhatók felhőszolgáltatással összefüggésben is, amikor a felhőszolgáltató adatfeldolgozó. A gyakorlatban a BCR felhő felhasználók és szolgáltatók között történő használata ritka, mert alkalmazhatóságuk vállalatcsoporton belüli adatfeldolgozásra korlátozódik.

SPECIÁLIS ADATKATEGÓRIÁK („KÜLÖNLEGES ADATOK”)

9

Hogyan definiálja az EU Adatvédelmi Irányelve a „különleges adat” fogalmát? Hogyan dolgozhatók fel a különleges adatok?

Az EU Adatvédelmi Irányelve rendelkezéseket tartalmaz az ún. „speciális adatkategóriák” feldolgozásáról, amelynek a következő fogalom-meghatározását adja: „faji vagy etnikai hovatartozásra, politikai véleményre, vallási vagy filozófiai nézetekre, szakszervezeti tagságra és az egészségre vagy a szexuális éltre vonatkozó adatok feldolgozása.” Ezek a speciális adatkategóriák (általában ezeket a „különleges adatok” (sensitive data) kifejezéssel illetik) csakis akkor kezelhetők, ha ahhoz vagy (i) az érintett kifejezett hozzájárulása rendelkezésre áll, vagy (ii) kifejezett hozzájárulás hiányában akkor, ha az EU Adatvédelmi Irányelvében meghatározott valamelyik speciális feltétel megvalósult. Az utóbbiak között van például az olyan adatkezelés, amely az adatkezelő munkajogi kötelezettségeinek a teljesítéséhez, illetve meghatározott jogai gyakorlásához; amely az érintett létfontosságú érdekei védelmében szükséges, vagy amely olyan adatra vonatkozik, amelyet az érintett kifejezetten nyilvánosságra hozott, vagy amely jogi igények megállapításához, jogok gyakorlásához vagy védelméhez szükséges, vagy ha az egészségügyi adatok feldolgozása egészségügyi szakdolgozó által orvosi vagy gyógyászati kezelés keretében történik.

Adattovábbítási szempontból a különleges adatok kezelése általában megegyezik bármilyen más személyes adatokéval (a határokon át történő adattovábbításról lásd a 7. és 8. kérdésre adott válaszokat). Ezt a következtetést támasztja alá az Európa Tanács az orvosi adatok védelméről szóló R (97) 5 számú ajánlásának 11. cikke, amely így rendelkezik: „az orvosi adatok határokon át történő áramlását olyan államba, amely csatlakozott az egyéneknek a személyes adatok automatikus feldolgozása során való védelméről szóló Egyezményhez, illetve amely kiadott jogszabályt az orvosi adatok legalább egyenértékű védelméről, nem helyes az adatvédelemre tekintettel különös feltételekhez kötni.” Az ajánlás leszögezi továbbá, hogy „ha az orvosi adatok védelme úgy ítélhető meg, mint amely összhangban van az Egyezményben lefektetett egyenlő védelem elvével, akkor nem helyes korlátozni az orvosi adatok határokon át történő áramlását olyan államba, amely nem ratifikálta ugyan az egyezményt, de rendelkezik olyan jogszabályokkal, amelyek biztosítják a védelmet az Egyezmény elveivel és a jelen ajánlással összhangban.”

Ha különleges adatok az EU Általános Szerződési Feltételek szerint továbbítandók olyan harmadik országokba, amelyek nem biztosítanak megfelelő

védelmet, akkor az adatexportőrnek kötelessége biztosítani azt, hogy az érintett a küldést megelőzően, vagy azt követően a lehető leghamarabb megkapja a tájékoztatást az adatai lehetséges továbbításáról olyan harmadik országba, amely nem biztosít megfelelő védelmet.

EGYÉB KÖVETELMÉNYEK

10

Megengedett-e, hogy egy felhőszolgáltató reklám céljára adatbányászati tevékenységet végezzen a felhasználó adatai tekintetében?

Nem. Személyes adatok minden esetben csakis meghatározott, egyértelmű és jogszerű célok érdekében dolgozhatók fel, és további feldolgozásuk nem megengedett olyan módon, amely nem egyeztethető össze azokkal a célokkal. Az adatkezelő (a felhő felhasználó) köteles meghatározni a feldolgozás egy vagy több célját, amikor a személyes adatokat az érintettől begyűjti, és arról köteles az érintettet tájékoztatni. A felhőszolgáltató csakis ilyen jóváhagyott célokra dolgozhat fel adatokat a felhő felhasználó utasításainak megfelelően.

11

Foglalja össze a főbb szempontokat azzal kapcsolatban, hogy Felhő Vélemény alapján a felhőszolgáltatók kötelesek magukat a felhasználóik számára átláthatóvá tenni.

Az átláthatóság főbb szempontjai a következők:

(i) A felhasználó, a felhőszolgáltató és az alvállalkozók (ha vannak ilyenek) közötti viszonyok; a felhasználót tájékoztatni kell minden alfeldolgozóról és minden olyan helyről, ahol adatfeldolgozás történhet (különösen, ha az az EGT-n kívül van), az alvállalkozásba adott szolgáltatás típusáról, a meglévő és a lehetséges alvállalkozók jellemzőiről, és azokról a garanciákról, amelyeket ezek az entitások a felhőszolgáltatónak nyújtanak az EU Adatvédelmi Irányelvének való megfelelés érdekében.

(ii) A szolgáltató által bevezetett technikai és szervezési intézkedések; a felhő felhasználót különösen arról kell tájékoztatni, hogy a felhasználó rendszerére telepített-e a felhőszolgáltató bármilyen szoftvert (pl. böngésző bekapcsolókat), és azok jelentőségéről adatvédelmi és adatbiztonsági szempontból.

12

Megfelel-e egy a felhőszolgáltató által választott független harmadik személy által lefolytatott audit annak a célnak, amelyre a felhő felhasználó egyedi átvilágítási joga szolgál?

Igen. A Felhő Vélemény elismeri azt, hogy egy sokügyfeles virtuális szerver környezetben hosztolt adatok egyedi kezdeményezésre történő átvilágítása technikailag célszerűtlen lehet, és olykor meg is növelheti az azon elhelyezett fizikai és logikai alapú biztonsági hálózati kontrollokat fenyegető kockázatokat. A Felhő Vélemény szerint ilyen esetekben az adatkezelő által választott harmadik személy által végzett audit tekinthető úgy, hogy az alkalmas az egyedi adatkezelő átvilágítási jogának a helyettesítésére. Feltétlenül szükséges azonban, hogy az ilyen audit független és átlátható legyen.

KÖZSZFÉRA

13

Vannak-e eltérő védelmi követelmények attól függően, hogy a felhő felhasználó a köz- avagy a magánszférához tartozik?

Nincsenek. Az EU Adatvédelmi Irányelve nem tesz különbséget a köz-, illetve a magánszférához tartozó adatkezelők (felhő felhasználók) között.

(i) A Felhő Vélemény jövőben várható fejleményekre tekintettel adott ajánlásaiban kifejti, hogy külön óvintézkedésekre lehet szükség, ha a közszféra kíván felhő megoldásokat alkalmazni. A közszféra szervezeteinek először fel kell becsülniük, hogy az adatoknak az állam területén kívülre történő kommunikálása, feldolgozása és tárolása elfogadhatatlan kockázatoknak teheti ki a polgárok és adataik biztonságát, a nemzetbiztonságot és a gazdaságot – különösen, ha azok érzékeny adatbázisokat (pl. választási adatok) és szolgáltatásokat (pl. egészségügy) érintenek. Külön megfontolást igényel, amikor különleges adatok feldolgozása történik felhő környezetben. A Felhő Vélemény ezzel kapcsolatban kifejti, hogy „ebből a szempontból a nemzeti kormányoknak és az EU intézményeinek megfontolás tárgyává kellene tenniük, hogy tovább vizsgálják az Európai Kormányzati Felhőről mint nemzetek feletti virtuális térről szóló elképzelést, ahol egy konzisztens és harmonizált szabályrendszer lenne alkalmazható.” A kormányzati felhők sajátosságait taglalja egy, a kormányzati felhők biztonságáról és rugalmasságáról szüle-

tett ENISA tanulmány is (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport), valamint a 2013. november 15-én kelt, a kormányzati felhők alkalmazásának bevezetésével kapcsolatos jó gyakorlatról szóló ENISA jelentés (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds/).

TÁJÉKOZTATÓK ÉS AJÁNLÁSOK

14

Az EU adatvédelmi hatóságainak milyen iránymutatásai állnak rendelkezésre a felhő alapú számítás-technikáról?

Lásd az alábbiakat:

(i) a WP 29 05/2012 számú véleménye (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf);

(ii) a WP 29 1/2010 számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

További iránymutatás található az alábbi anyagokban:

(iii) Munkaanyag a felhő alapú számítástechnikáról – adatvédelmi kérdések („Sopot Memorandum"), amelyet a Távközlési Adatvédelemmel Foglalkozó Nemzetközi Munkacsoport (International Working Group on Data Protection in Tele-communications) adott ki 2012. április 24-én (http://germanitlaw.com/wp-content/uploads/2012/04/Sopot-Memorandum1.pdf)

(iv) Felhő alapú számítástechnikai kockázatelemzés, amelyet az EU Hálózati és Információs Biztonsági Ügynöksége (European Union Agency for Network and Information Security – ENISA) adott ki 2009. november 20-án (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment)

15

Melyek a WP 29 által a felhő felhasználók részére a Felhő Véleményben adott főbb ajánlások?

A WP 29 által felhő felhasználók számára adott főbb ajánlások a következők:

(i) Átfogó és alapos kockázatelemezést kell végezni a cloud computing alkalmazása; az adatvédelemmel kapcsolatos jogi kockázatokra különösen oda kell figyelni, azon belül főként a biztonsági kötelezettségekre és a nemzetközi adattovábbításokra;

(ii) Átláthatóságot kell biztosítani. A felhő felhasználót minden alvállalkozóról tájékoztatni kell, amelyek az egyes felhő szolgáltatások nyújtásában segédkeznek, továbbá minden helyről, ahol személyes adatok tárolása vagy feldolgozása történhet (különösen, ha az az EGT-n kívüli hely). Ilyen alfeldolgozásra kizárólag a felhasználó előzetes jóváhagyásával kerülhet sor. A felhasználónak érdemi információt kell kapnia a felhőszolgáltató által bevezetett technikai és szervezési intézkedésekről;

(iii) A felhasználónak biztosítania kell, hogy érvényesül a célhoz kötött adatkezelés elve, vagyis a személyes adatokat kizárólag a felhasználó mint adatkezelő által meghatározott célból dolgozzák fel.

ORSZÁGONKÉNT ELTÉRŐ RENDELKEZÉSEK
A HELYI ADATVÉDELMI JOGSZABÁLYOK ALAPJÁN

MAGYARORSZÁG

ÜGYVÉDI ELÉRHETŐSÉGI ADATOK:

Ország:	Magyarország
Ügyvédek:	Petrányi Dóra, Domokos Márton
Ügyvédi Iroda:	CMS Cameron McKenna LLP H-1053 Budapest Károlyi utca 12. Magyarország
Website:	www.cms-cmck.com
E-mail:	communications@cms-cmck.com

Az alábbi összefoglaló vázlatosan ismerteti a szektortól független követelményeket, amelyeket szervezeteknek és intézményeknek szem előtt kell tartaniuk, ha cloud computing-ot kívánnak igénybe venni. Kérjük, tanulmányozza együtt az alábbi táblázatot az EU adatvédelmi joga szerinti követelményeket ismertető táblázattal (lásd fent).

BEVEZETÉS

1

Mi az általános jogszabályi alapja a személyes adatok védelmének?

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (az „Adatvédelmi Törvény"). Az Adatvédelmi Törvény néhány kivétellel (mint pl. az adatfeldolgozó definíciója, a Kötelező Erejű Vállalati Szabályok elismerésének hiánya, a jogos érdeken alapuló adatkezelés definíciója) lényegében megegyezik az EU Adatvédelmi Irányelvével. Az Adatvédelmi Törvény az alábbi link segítségével érhető el: www.naih.hu/files/Infotv-_MO.pdf.

2

Mely hatóság felügyeli az adatvédelmi jogok érvényesülését? Foglalja össze a jogköreit.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: „NAIH"). A weboldala a következő: www.naih.hu.

Címe: H-1125 Budapest, Szilágyi Erzsébet fasor 22/C

A NAIH autonóm államigazgatási szerv, amelynek hatásköre az Adatvédelmi törvény rendelkezési betartásának felügyelete. A NAIH jogosult vizsgálatokat folytatni (beleértve helyszíni vizsgálatot is), határozatban megállapítani az Adatvédelmi Törvény megsértését, valamint bírságot kiszabni és egyéb intézkedéseket hozni jogszabálysértés esetén. A NAIH fogadja és megválaszolja a panaszokat az Adatvédelmi Törvény megsértésével kapcsolatban. A NAIH adatvédelmi nyilvántartást vezet, és konzultációt is végez a személyes adatok védelme területén. Általánosságban a NAIH csak Magyarországon letelepedett felhőszolgáltatók és felhő-felhasználók tekintetében rendelkezik hatáskörrel. A NAIH akkor is hatáskörrel rendelkezik egy adatkezelés tekintetében, ha az Magyarország területén történik, és az adatkezelő – felhő-felhasználó – az EU területén kívül telepedett le (pl. az USA-ban), de az adatkezelést Magyarország területén végzi.

Figyelembe véve az eddigi hatósági gyakorlatot (nevezetesen egy szlovákiai társaság ellen hozott döntést), valamint a NAIH 2013. évi Éves Jelentésében foglalt megállapításait, úgy tűnik, hogy a NAIH az Adatvédelmi Törvény hatályának kiterjesztő értelmezésére törekszik, azaz olyan értelmezésre, amely feljogosítja olyan szolgáltatók felügyeletére is, akik külföldiek ugyan, de adatfeldolgozási műveleteket végeznek magyarországi természetes személyek részére értékesített termékek és szolgáltatások tekintetében. Ennek a kiterjesztő értelmezésnek a jogszerűségét jogszabály vagy bíróság (ahova a NAIH döntése ellen jogorvoslattal fordultak) még nem erősítette meg.

3

Jelölje meg a helyi adatvédelmi jogszabályok alkalmazhatóságának követelményeit.

A követelmények egy kivétellel megfelelnek az EU Adatvédelmi Irányelvében foglalt, az EU Adatvédelmi Jogszabályáról szóló részben a 2. kérdésre adott válaszban ismertetett rendelkezéseknek. Az Adatvédelmi Törvény hatálya minden adatkezelési műveletre kiterjed, amelyet Magyarországon végeznek, ha az személyes adatokat érint. A magyar

jog akkor is alkalmazandó az adatkezelésre, ha azt Magyarországon végzik, de egy külföldi adatkezelő tevékenységének keretében. Ez a megközelítés szigorúbb, mint az EU Adatvédelmi Irányelv 4. cikke, valamint a WP 29-nek az alkalmazandó jogról szóló 8/2010. számú véleményében meghatározott álláspontja.

FELHASZNÁLÓ / FELHŐSZOLGÁLTATÓ / ALADATFELDOLGOZÓ – FELADATOK ÉS FELELŐSSÉGI KÖRÖK

4

Vannak-e olyan, a helyi jogszabályok által előírt követelmények az adatfeldolgozás és az adatfeldolgozási megállapodások tekintetében, amelyek túlmutatnak az EU Adatvédelmi Irányelvének követelményein?

Igen. Az Adatvédelmi Törvény az alábbi, meglehetősen szigorú felelősségi szabályt tartalmazza az adatkezelő (felhő-felhasználó) tekintetében: ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni. Az érintettel szemben az adatkezelő felel az adatfeldolgozó (pl. felhőszolgáltató) által okozott kárért. Az adatkezelő akkor mentesül az okozott kárért való felelősség alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

A NAIH részletesen meghatározza az EU Adatvédelmi Irányelvének az írásbeli – az adatkezelő és az adatfeldolgozó által minden egyes adatfeldolgozási viszony céljára megkötendő – adatfeldolgozási megállapodásról szóló általános követelményeit. Az Adatvédelmi Törvény nem ír elő minimális tartalmi követelményeket az ilyen megállapodásokra. Ugyanakkor NAIH azt ajánlja, hogy az adatfeldolgozási megállapodások tartalmazzák legalább (i) a felek konkrét tevékenységeit, döntéshozatali jogaikat és azok korlátait, (ii) az adatkezelőnek azt a lehetőségét, hogy biztonsági auditot folytathasson le, és az ehhez kapcsolódó formai követelményeket / dokumentációt (az elkészítés oka, az elkészítés célja, hiányosságok orvoslásakor a felelősség és a feladatok meghatározása stb.), (iii) részletes együttműködési kötelezettséget, különösen adatbiztonsági esemény bekövetkezése vagy adatlopás esetén (pl. kríziskezelés, hibajavítás, további veszteségek bekövetkezésének megelőzése, pontos határidők meghatározása, stb.), (iv) adatok megtartására / törlésére vonatkozói kötelezettségeket és (v)

az adatfeldolgozási viszony megszűnése után is hatályban maradó, „túlélő rendelkezéseket”.

Az adatkezelő, illetve az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó – jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező – belső adatvédelmi felelőst kell kinevezni vagy megbízni

a) az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál;

b) a pénzügyi szervezetnél;

c) az elektronikus hírközlési és közüzemi szolgáltatónál.

Más szervezetekben az adatbiztonsági felelős személy kinevezése önkéntes. Az ún. „belső adatvédelmi felelősök konferenciája” rendszeres szakmai párbeszédet folytat az adatvédelmi felelősök és a NAIH között.

5

Az Adatvédelmi Törvényben szabályozott technikai és szervezési intézkedések felsorolása, ha van ilyen.

Az EU Adatvédelmi Irányelv VIII. részében foglalt követelményeken túl az Adatvédelmi Törvény megköveteli, hogy a személyes adatokat védeni kell az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve ha azt törvény lehetővé teszi –, közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

Személyes adatok automatizált feldolgozása esetére további biztonsági intézkedések és biztosítékok alkalmazandók. Az Adatvédelmi Törvény nem határozza meg annak a konkrét módját, hogy miként kell az előbb említett általános kötelezettségeknek teljesülnie (pl. egy bizonyos technológia használatával). Az adatfeldolgozás során alkalmazandó biztonsági intézkedésekről való döntéskor az adatkezelőknek és – feldolgozóknak figyelembe kell venniük a legfrissebb technológiai vívmányokat, és a technika állását azok bevezetésekor. A NAIH nyilvánosság számára elérhető vizsgálatai iránymutatásként szolgálnak

a technológiai és szervezeti intézkedések megfelelőségének értékelésekor: amikor a NAIH ellenőrzi az adatfeldolgozók szóban forgó intézkedéseit, különösen az alábbiakat vizsgálja: a hozzáférési jog gyakorlásához előírt eljárások, az adatkérések naplózása és az adatkezelés nyilvántartásba vétele.

A személyes adatokat védeni kell természeti csapások, műszaki hibák és jogellenes emberi magatartások ellen (szándékos adatsértés, hanyagság, mulasztás). A belső nyilvántartásokat egymástól külön kell tartani. Meg kell akadályozni a jogellenes hozzáférést a személyes adatokhoz, továbbá az adatátvitelnek és adatfelvételeknek visszakövethetőknek kell lenniük (naplózás). Működési hiba esetén adat-helyreállításnak kell rendelkezésre állnia, és minden adathozzáférést és hibát dokumentálni kell. Biztonsági mentési másolatokat kell készíteni, és a biztonsági eseményeket jelenteni kell belső elemzés érdekében.

NEMZETKÖZI ADATTOVÁBBÍTÁSOK

6

Előírja-e helyi jogszabály vagy rendelkezés az Adatvédelmi Hatóság részére való bejelentést vagy jóváhagyásának kikérését az EU Általános Szerződési Feltételek vagy az EU-US Biztonságos Kikötő Keretszabályok alapján az EGT-n kívülre történő adattovábbítást?

Nem. Alakszerű NAIH jóváhagyás, és bejelentés sem szükséges.

7

Írja le azokat a követelményeket, amelyek személyes adatoknak az EGT-n kívülre történő továbbítása esetén túlmutatnak az EU Adatvédelmi Irányelvében foglalt követelményeken.

A Kötelező Erejű Vállalati Szabályokat Rendelkezéseket Magyarországon nem szabályozzák és nem ismerik el.
Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény további korlátozásokat tartalmaz: a kormányzati szervek és önkormányzatok által, valamint ezen szervek

széles köre számára végzett adatfeldolgozás (beleértve a legtöbb hatóságot, minisztériumot, a fegyveres testületeket és az önkormányzatokat) kizárólag Magyarország területén végezhető, vagy egy zárt IT rendszerben diplomáciai célokra, kivéve, ha (i) a külföldön történő feldolgozást a felügyeleti szerv vagy nemzetközi egyezmény megengedi, és (ii) az adatfeldolgozás az EU területén történik. Európai vagy nemzeti kritikus infrastruktúra (amint azt a jogszabály meghatározza) katonai működtetésű kormányzati elektronikus információs rendszerével kapcsolatos adatfeldolgozás lehetséges a felügyeleti szerv engedélye vagy nemzetközi egyezmény felhatalmazása nélkül is, ha az egy másik EU tagországokban történik.

SPECIÁLIS ADATKATEGÓRIÁK („KÜLÖNLEGES ADATOK”)

8

Vannak-e olyan helyi követelmények különleges adatokkal kapcsolatban, amelyek eltérnek az EU Adatvédelmi Irányelvének követelményeitől?

Nincsenek. A szabályok és a követelmények többnyire követik az EU Adatvédelmi Irányelvében foglaltakat. Általánosságban írásbeli jóváhagyás szükséges különleges személyes adatok kezeléséhez (kivéve, ha az adatkezelést jogszabály írja elő), ugyanakkor az Adatvédelmi Hatóság elfogadja a jóváhagyást érvényesnek akkor is, ha az elektronikus úton történt, és az érintett egyértelműen azonosítható.

PÉNZÜGYI ADATOK

9

Foglalja össze röviden a pénzügyi adatokra alkalmazandó fő szektorspecifikus jogi és szabályozási követelményeket, amelyeket a hitelintézeteknek ismerniük kell, ha felhő szolgáltatást kívánnak igénybe venni, ha vannak ilyenek.

A Pénzügyi Szervezetek Állami Felügyelete (PSZÁF – jogutóda a Magyar Nemzeti Bank, a továbbiakban együtt: „MNB”) a 4/2012. szám alatt 2012. július 18-án kibocsátott Vezető Körlevele a pénzügyi szervezeteknél a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról a felhő alapú szolgáltatás igénybevételét kiszervezésnek nyilvánítja, függetlenül a felhő alapú szolgáltatás pontosan meghatározott természetétől. Ennek eredményeként a hitelintézetekről és pénzügyi vállalkozásokról

szóló 2013. évi CCXXXVII. törvény kötelező rendelkezései betartását biztosítani kell, beleértve a felhő szolgáltatási (kiszervezési) megállapodás néhány kötelező elemét. A kiszervezési (felhő) megállapodásban az alábbi főbb rendelkezéseknek kell szerepelniük:

(i) A kiszervezett tevékenységek pontos körének világos meghatározása és adatvédelmi intézkedések.

(ii) A hitelintézetnek, a belső ellenőrzésnek, a külső könyvvizsgálónak, valamint az MNB-nek a helyszíni és helyszínen kívüli ellenőrzéshez való joga. Jogszabálysértés vagy a felhő szolgáltatási megállapodás megszegése esetén a hitelintézet jogosult értesíteni az MNB-t.

(iii) A hitelintézet jóváhagyási jogának rögzítése alvállalkozásba (alfeldolgozásba) adáshoz, a tevékenységnek az MNB és a hitelintézet belső ellenőrzése, könyvvizsgálója által történő ellenőrzési joga.

(iv) A felhőszolgáltató kötelezettsége a felhő szolgáltatások megfelelő g ondosság mellett történő nyújtására, és rendkívüli felmondási jog a hitelintézet javára az adatfeldolgozási megállapodásnak a felhőszolgáltató által való súlyos vagy ismételt megszegése esetén.

(v) A felhő szolgáltatások minőségének részletes paraméterei (szolgáltatási szint megállapodás).

(vi) Bennfentes kereskedelem tilalmára vonatkozó kötelező törvényi rendelkezések beemelése.

(vii) „Érdekellentét kizárása", azaz kötelezettség a felhasználó adatainak elkülönítésére más felhasználók adataitól, ha a felhőszolgáltatónak egynél több ügyfele van.

A hitelintézetet köteles a felhőszolgáltatót az általános szerződési feltételeiben megnevezni.

Lényegében hasonló kötelezettségek terhelik a biztosító társaságokat és a befektetési szolgáltatókat az irányadó szektorális jogi szabályozás alapján.

10

Van-e bejelentési kötelezettség a szabályozó hatóság részére, illetve szükséges-e a szabályozó hatóságtól jóváhagyást kérni felhő szolgáltatás igénybe vételéhez?

Igen. A hitelintézet köteles a kiszervezési (felhő-) szolgáltatási szerződés aláírását követő 2 napon belül bejelenteni az MNB-nek (i) a kiszervezés tényét; (ii) a felhőszolgáltató nevét és címét; és (iii) a kiszervezés időtartamát. Lényegében hasonló kötelezettségek terhelik a biztosító társaságokat és a befektetési szolgáltatókat is.

EGYÉB KÖVETELMÉNYEK

11

Fejtse ki, ha az Adatvédelmi Törvény alapján megengedett, hogy egy felhőszolgáltató reklám céljára adatbányászati tevékenységet végezzen a felhasználó adatai tekintetében?

Nem megengedett. A célhoz kötött adatkezelés elve alkalmazandó, amint az az EU Adatvédelmi Jogszabályáról szóló rész 10. kérdésre adott válaszban kifejtésre került.

12

Követelmény-e az Adatvédelmi Törvény alapján, hogy a felhőszolgáltató ahhoz hasonlóan átlátható legyen, ahogyan a 11. kérdésnél kifejtésre került az EU Adatvédelmi Irányelve alapján?

Igen. Az EU Adatvédelmi Jogszabályáról szóló rész 11. kérdésre adott válaszban foglalt elvek alkalmazandók.

TÁJÉKOZTATÓK ÉS AJÁNLÁSOK

13

Van-e a Felhő Véleményen kívül olyan helyi útmutatás a felhő alapú számítástechnikáról, amelyet az Adatvédelmi Hatóság bocsátott ki?

Igen. Lásd a Pénzügyi Szervezetek Állami Felügyelete (PSZÁF) 4/2012. szám alatt 2012. július 18-án kibocsátott Vezetői Körlevelét a pénzügyi szervezeteknél a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról (csak magyar nyelven olvasható a Magyar Nemzeti Bank – a PSZÁF jogutóda – honlapján. http://felugyelet.mnb.hu/data/cms2364896/vezkorlev_4_2012.pdf).

Az Adatvédelmi Hatóság a cloud computing-gal kapcsolatban az Adatvédelmi Törvény alapján eddig kevés iránymutatást adott ki. 2012. évi Éves Jelentésében az Adatvédelmi Hatóság hangsúlyozta, hogy maga is a Felhő Véleményre és a Sopot Memorandumra támaszkodik, továbbá hogy „különleges adatok" felhőben való tárolása nem ajánlott (de nem is tiltott). A 2012. évi Éves Jelentés csak magyar nyelven olvasható az Adatvédelmi Hatóság honlapján – http://www.naih.hu/files/NAIH-2012-Beszamoloja-vegleges-web.pdf.

JOGSZABÁLYTERVEZETEK

14

Van-e olyan jogszabály-tervezet, amely lényeges hatással lesz a felhő szolgáltatásra?

Nincs.