PÉNZÜGYI SZERVEZETEK
ÁLLAMI FELÜGYELETE
HUNGARIAN FINANCIAL
SUPERVISORY AUTHORITY

4/2012. számú Vezetői körlevél

a pénzügyi szervezeteknél a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról

A Pénzügyi Szervezetek Állami Felügyelete (**Felügyelet**) az információ-technológia fejlődése, a virtualizáció és a felhőszolgáltatások (cloud computing services) elterjedése, valamint vizsgálati tapasztalatai alapján az alábbiakra hívja fel a felhőszolgáltatásokat igénybe vevő, vagy azt fontolgató pénzügyi szervezetek figyelmét.

Amennyiben egy intézmény felhőszolgáltatást vesz igénybe, az kiszervezésként kezelendő, amelyre az egyes ágazati jogszabályok tartalmazzák az irányadó követelményeket.

Ugyancsak az intézmény mindenkori felelőssége, hogy az általa végzett tevékenységgel arányos kockázatokat felmérve, annak tudatában és ismeretében válasszon új szolgáltatót, illetve technikai megoldást. A megvalósítás technológiai és szerződéses részleteinek jogszabályi megfelelőségét a Felügyelet helyszíni vizsgálatai során ellenőrzi.

A Felügyelet kiemelten felhívja az intézmények menedzsmentjének, az Informatikai Belső Ellenőrzésnek, a Compliance területnek, valamint a jogi területeknek a figyelmét arra, hogy amennyiben az adott intézmény felhőszolgáltatást kíván igénybe venni, úgy fordítsanak kiemelt gondot az alábbiakra:

- a felhőszolgáltatást érintő európai uniós jogszabály változások, gyakorlatok, „best practice” javaslatok folyamatos követése;
- a magyar és európai uniós adatvédelmi előírások, adatvédelmi gyakorlat – különös tekintettel a határokon keresztül megvalósuló, vagy harmadik országba irányuló adattranszferekkel kapcsolatos gyakorlatokra, állásfoglalásokra – folyamatos követése;
- a megkötendő szolgáltatási főszerződés és a kapcsolódó szolgáltatási szintre vonatkozó szerződések (**SLA**-k) egymáshoz való viszonya, tartalma – figyelemmel az alábbi 2. pontban felsoroltakra is.

1. **Adatok a** közösségi vagy publikus **felhőben**[1]
   1.1. **Adatosztályozás után lehet eldönteni**, hogy a kezelt adatok mely köre vihető egyáltalán publikus felhőbe. **Banktitkot, személyes vagy más érzékeny adatot a jelenlegi európai gyakorlat szerint nem ajánlott publikus felhőben kezelni** (banknál csak titkosított formában történő e-mail archiválásra van publikus felhő példa, Spanyolországban). Jellemzően az egy cégcsoporthoz tartozó leányvállalatok közösségi felhője létezik, illetve nagyon kis vállalatok fordulnak felhőszolgáltatókhoz (**Cloud Service Provider-CSP**). A publikus felhőben az adatok fizikai tárolásának

[1] privát felhő: egy cég –jellemzően virtualizált számítógépes környezetben– saját magának szolgáltat informatikai infrastruktúrát (Infrastructure as a Service: IaaS), fejlesztési platformot (Platform as a Service: PaaS) vagy szoftvert is (Software as a Service: SaaS); publikus felhő: a fenti szolgáltatástípusok bármelyikét egymástól független ügyfeleknek nyújtja egy CSP (pl. Gmail szolgáltatás); közösségi felhő: jellemzően egy cégcsoporthoz tartozó ügyfeleknek szolgáltat egy CSP, amely akár ugyanannak a cégcsoportnak is lehet a tagja.

vagy feldolgozásának helye (különösen pl. EGK-n vagy safe harboron[2] kívül) alapvetően befolyásolja az EU-n belüli adatvédelmi előírásoknak való megfelelés törvényi lehetőségét.

1.2. **Szerződéskötés előtt** javasoljuk az ún. **„Sopot Memorandum”** (EU adatvédelmi biztosok kiadványa) és az ENISA (az EU hálózatbiztonsági szervezete) dokumentumait, illetve a BSI (német információ biztonsági hivatal) biztonsági minimum követelményeit alapul véve **legalább az alábbi kockázatokat** mérlegelni és megfontolni:

1.2.1. vannak olyan **technológiai védelmi lehetőségek,** amelyek a felhőszolgáltatás alapját képező virtualizált környezetben **még nem képesek** a fizikai megfelelőjükkel azonos biztonsági szintet nyújtani (pl. virtuális hálózati védelem, teljes titkosítás a felhőben kezelt adatokra);

1.2.2. **digitális nyombiztosítás** (forensic) **és incidenskezelés** szempontjából: ha publikus CSP-hez tartozó ügyfeleket támadás ér, a támadó lehet a CSP másik ügyfele vagy maga a CSP is, ilyen esetben nehéz a naplóadatokból kideríteni pontosan mi történt. (pl. logok hozzáférhetősége, sértetlenségének biztosítása; a feltételezett támadó virtualizált gépének törlésével a naplóadatok is elvesznek, de megőrzéséhez nincs joga a CSP-nek, mert adatvédelmi jogszabályba ütközhet – erre megoldás lehet a fájlként titkosított *snapshot*, amelyet digitálisan aláírva megőriznek.);

1.2.3. azt a **folyamatot, amit az intézmény maga sem tud** megfelelő kontrollok mellett biztonságosan működtetni, megfelelő kontrollok nélkül nem javasolt CSP-hez kiadni (ez ahhoz hasonlít, mintha egy rosszul irányított folyamat javulását pusztán attól várnánk, hogy informatikai rendszert illesztünk rá);

1.2.4. a szolgáltató adja meg az **adatfeldolgozás lehetséges helyszínei**t – ez a vonatkozó országok jogszabályi környezete miatt fontos, lehetőleg kerülendő, hogy az EU-n, vagy a safe harbor-on kívüli helyre kerülhessenek adatok;

1.2.5. az **adattovábbítás és tárolás** korszerű titkosítással történjék, emellett az adatokhoz való **távoli hozzáférés** (jellemzően Interneten keresztül) korszerű azonosító technológián alapuljon (pl. kétfaktorú, erős kriptográfiával működő azonosítás);

1.2.6. **elvárt a biztonsági naplózás** az adatok helymeghatározása, másolása és törlése, illetve mindenféle típusú hozzáférése szerint;

1.2.7. az **adatok törlése** biztonságos módszerrel, azaz a törlendő adat helyének véletlenszerű adatokkal történő (többszörös) felülírása révén történjék.

2. A **bizalom és az átlátható, biztonságos működés** záloga a **szerződés** marad, így az abban foglaltak különösen fontosak, mint például:

2.1. **a főszerződés és az SLA, vagy SLA-k** folyamatos **monitorozása** és az aktív visszacsatolás garanciái (pl. a felügyelt intézmény biztonsági előírásainak/szabályzatának beemelése a szerződés egyik mellékletébe, úgy, hogy a felügyelt intézmény számára folyamatosan ellenőrizhető lehessen annak betartása, lásd bővebben az ENISA Procure Secure anyagát);

2.2. az intézményeknek célszerű arra is kiemelt gondot fordítani, hogy a főszerződés és az SLA-k definíciói, terminológiája ne térjen el egymástól, **egységesen alkalmazzák a fogalmakat**;

2.3. ugyancsak nem ajánlott blankettaszerződéseket, általános szerződési feltételeket alkalmazni, (különös tekintettel a nem magyar jog alatt készült mintákra);

[2] *safe harbor* alá jelentkeznek be azon amerikai vállalatok, amelyek ezzel vállalják, hogy az európai adatvédelmi szintnek megfelelően kezelik a személyes adatokat

2.4. a szolgáltatónak való kiszolgáltatottságot elkerülendő olyan feltételek meghatározása a szerződésben, amelyek nem nehezítik meg a **szolgáltató váltást** (a szerződés felmondásának lehetősége, az adatokhoz történő mindenkori szabad hozzáférés biztosítása olyan adatformátumban, amely biztosítja az adatok hordozhatóságát);

2.5. **magas rendelkezésre állási** kontrollok (pl. földrajzilag elkülönült, hibatűrő módon konfigurált, fürtözött szerverek, adattárolók a virtuális szerverek gazdagépeként) és kiváló **DRP** (helyreállítási terv) **készültség** (az ügyfél üzletmenet folytonossági tervéhez illeszkedő, életszerű helyreállítási tervek és azok hiteles tesztjei, teszteléssel kapcsolatos felelősségek meghatározása);

2.6. erős **incidenskezelési** eljárások (az ügyfél azonnali és minél teljesebb körű tájékoztatása);

2.7. mennyire rugalmasan tudja kiszolgálni a változó **kapacitásszükségletet** a CSP (pl. időszakos csúcsterhelés esetén gyors erőforrás allokáció vagy épp ellenkezőleg, csökkenő igényekhez gyorsan igazodó rugalmas árazás);

2.8. **változáskezelési kontrollok** szabályozása, gyakorlati alkalmazása és ellenőrzése (pl. annak meghatározása, hogy melyek azok a szolgáltatás minőségét érintő változások, amelyekről haladéktalan ügyfél tájékoztatás szükséges);

2.9. **független auditok** a CSP üzleti és biztonsági érdekeinek figyelembe vételével az ügyfél számára elérhetővé tett tartalommal (pl. sérülékenységi vizsgálatok, behatolási tesztek kívülről és a virtualizált környezeten belül, az ügyfelek között is), és **biztonsági tanúsítások** (pl. ISO 27001, SAS70v2:ISAE3402, PCI DSS). Ugyanakkor nehéz olyan auditort vagy szakjogász találni, aki kellő tapasztalattal rendelkezik a virtualizált környezettel kapcsolatban. A biztonság nem egy tanúsítvány megszerzése szempontjából fontos cél, sokkal inkább egy önjavító folyamat által fenntartott állapot;

2.10. **rendelkezések a szerződő felek vitája** esetére (irányadó jogrend és illetékes vitarendezési fórum meghatározása), illetve **hatósági megkeresés** esetén (ügyféladatok kiadásának feltételei);

2.11. a **felelősségi és biztosítéki szabályok precíz kidolgozása** és a magyar jogintézményekhez való illesztése, érvényesíthetőségének biztosítása (felelősségek tisztázása, felelősségkizáró klauzulák mellőzése, a biztosítékok között a szolgáltató felelősségbiztosítása terhére történő helytállásnak, bankgarancia adására vonatkozó kötelezettségnek a beemelése a szerződésbe, stb.).

(Hasznos linkek a cloud computing és a virtualizáció technológiai és szabályozási vonatkozásairól a következő oldalakon.)

- Neelie Kroes adatvédelmi törvény javaslatáról szóló ismertető: https://cloudsecurityalliance.org/wp-content/uploads/2012/02/GILBERT-Draft-EU-Regulation-2012-02-08.pdf
- és az EU felhőstratégiájának beharangozója: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50
- a Sopot Memorandum (a pénzügyi szektor is hasonló biztonsági szinten működő telco iparágnak készítette az európai adatvédelmi felelősökből álló Berlini Csoport): http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083
- az ISACA ellenőrzési irányelvei (itt csak tartalomjegyzék és az első két fejezet, de ISACA-tagok számára ingyenesen letölthető az egész szöveg): http://www.isaca.org/Knowledge-Center/Research/Documents/ITCO_Cloud_SAMPLE_E-book_20July2011.pdf
- az ENISA 2009. évi cloud kockázatelemzése, ellenőrzési irányelvei és körképe a KKV szektorról: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing
- 2011. júniusában Budapesten volt nemzetközi adatvédelmi konferencia (http://www.eu2011.hu), ezen az ENISA álláspontját is kifejtették a cloudról: http://www.eu2011.hu/files/bveu/documents/Slawomir_Gorniak_-_Cloud_computing_-_Security_and_privacy_issues.pdf
- ugyancsak az ENISA 2012. évi tanulmánya a biztonsági SLA monitorozásának irányelveiről: http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
- illetve a közszférában e téren tapasztaltakról szóló ENISA elemzés: http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector
- a CSP-ekkel szembeni biztonsági elvárások tekintetében az egyik legátfogóbb és legkidolgozottabb megközelítés a német információbiztonsági államhivataltól (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.html;jsessionid=C471291603DD7CF51CEC200B8F888650.2_cid244
- az EuroCloud tanúsítvány kezdeményezés kiadványai: http://www.saas-audit.de/en/certification/at-a-glance/

  (a contract template-ben utalnak egy audit questionnaire-re, amint kész lesz, biztos érdekes felvetéseket hoz),
- az EuroCloud akciótervének 16 pontja: http://www.eurocloud.org/wp-content/uploads/2011/04/EuroCloud-16-PointForCloudComputingInEurope_rev1.pdf
- a Cloud Security Alliance a szolgáltatói oldal önszabályozása keretén belül állapít meg tanúsítvány/audit kritériumokat : https://cloudsecurityalliance.org/research/initiatives/ccm/
- és az audit munkacsoportjuk is aktív: https://cloudsecurityalliance.org/research/initiatives/cloudaudit/
- a PCI DSS 2.0-hoz is kiadott virtualizációs kiegészítést (ami nem azonos a számítási felhő koncepcióval, de annak alapját képezi): https://www.pcisecuritystandards.org/documents/Rth87Wp/Virtualization_InfoSupp_v2.pdf

- Az egyesült államokbeli szabványügyi hivatal (NIST) kiadványai szintén a sztenderdizálás felé tett lépéseket tükrözik:
- http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
- http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024
- http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf

Budapest, 2012. július 18.

Dr. Szász Károly
a PSZÁF elnöke