FELHŐ ALAPÚ SZÁMÍTÁSTECHNIKA A MAGYAR ADATVÉDELMI KÖRNYEZETBEN

Készítette:
Advanced Network Technologies Kft
2013

1. Általában a felhőszolgáltatás és a jog kapcsolatáról

A hagyományos jogi gondolkodás és jogi intézmények rendszerében az alapfogalom a „dolog” volt, eredeti és legszűkebb értelmében a „birtokba vehető testi tárgy”. Éppen ezért a jog számára már az is komoly kihívást jelentett, amikor a pénz (amely bankjegyként már nem fizikai mivoltában hordozta a lényegét), vagy a nem megragadható erőforrások (tipikusan az elektromos áram) vonatkozásában is értelmezhetővé kellett tegye a dolog fogalmát és általában a hagyományos jogi logikát.
Egészen újszerű problémakörrel szembesült azután a jogalkotás akkor, amikor az informatikára kellett átültesse addigi fogalmi rendszerét, hiszen az informatika – túl a bizonyos értelemben egyre inkább háttérbe szoruló hardver elemeken – semmiféle „kézzelfogható”, a hagyományos jogfogalmakkal pontosan körülírható összetevőt nem tartalmazott.
Az informatikai szolgáltatásokra kezdettől fogva jellemző volt, hogy többnyire a klasszikus szerződéstípusok (pl. adásvétel, bérlet, megbízás, vállalkozás) egyikébe sem voltak besorolhatók, s ahogyan a szolgáltatások komplexitása rohamosan nőtt (a szolgáltató nem egyszerűen hardvert ad el, vagy ad bérbe, hanem azon szoftvert biztosít, ahhoz támogatást nyújt stb.), úgy nőtt a távolság is a korábbi jogi környezet és az informatika támasztotta igények között.
A fenti folyamatban újabb döntő változást jelentett az internet térhódítása, amelynek eredményeként nemcsak a nyújtható szolgáltatások tárgya vált még nehezebben megragadhatóvá, de egyik pillanatról a másikra még azt is kérdésessé tette, hogy egyáltalán kik az alanyai egy bizonyos jogviszonynak. A jog számára ugyanis evidens volt, hogy a szerződéses kapcsolat értelemszerűen tartalmazza a felek pontos meghatározását, ez azonban az interneten hozzáférhető szolgáltatásokra létrejött szerződésekben már másodlagossá vált: a felhasználó számára sokszor nem szempont, hogy az adott szolgáltatást milyen szervezet nyújtja, megismerhető, elérhető-e, s lehetséges-e pl. vele bármiféle jognyilatkozatot közölni. A felhasználó oldaláról nézve tehát egyes esetekben „eltűnt”, de legalábbis eltávolodott a szolgáltató. Ezt erősítette természetesen az a jelenség, hogy rendkívül rövid idő alatt tömegessé váltak – még a mindennapi, kisebb jelentőségű ügyletekben is – a nemzetközi elemet tartalmazó, tehát a nemzeti határok és jogrendszerek létét figyelmen kívül hagyó szerződések.

Ami a felhőszolgáltatásokat illeti (különös tekintettel a publikus felhőre, amely interneten érhető el), ezek minden olyan sajátosságot, amely a jogi szabályozás számára az informatika területén nehézséget okoz, magukban hordoznak, sőt bizonyos tekintetben ezeket a problémaköröket még mélyítik és tágítják. Ennek hátterében a felhőszolgáltatások közös jellemzője áll: a szolgáltatások fokozott virtualizációja, amelyben éppen az az egyik alapvető szolgáltatási jellemző, hogy a felhasználó számára – többé vagy kevésbé – távoli és ismeretlen (mindenesetre a felhasználó által nem vagy alig kontrollálható) erőforrásokat nyújt, amelyek kulcsa a szinte korlátlan kapacitás, rendelkezésre állás és hozzáférés, függetlenül helytől, időtől, felhasználók számától. Természetesen privát felhő esetében, tehát saját vagy bérelt erőforrásokra támaszkodva a szolgáltatás kevesebb, illetve jobban kezelhető jogi problémát vet fel, de egy területen mindenképpen kiélezi a már eddig sem ismeretlen szabályozási és jogalkamazási ellentmondásokat: ez pedig az adatvédelem.

Attól kezdve ugyanis, hogy egy felhasználó valamilyen mértékben külső erőforrásra támaszkodik (különösen infrastruktúra, vagy platform szolgáltatás esetén), a felhasználóhoz kapcsolódó adatok szükségszerűen kikerülnek a felhasználó teljes ellenőrzése alól. A jelen tanulmány célja annak összefoglaló jellegű bemutatása, hogy *az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény* (a továbbiakban: **Infotv.**) tükrében a felhőszolgáltatások milyen adatvédelmi kérdéseket vetnek fel, azzal a szűkítéssel azonban, hogy a nemzetközi elemet tartalmazó felhőszolgáltatások elemzését mellőzzük, hiszen azok esetében az egyéb – vizsgálatunk tárgyát nem képező – nemzeti jogok és uniós szabályozók lehetnek (részben) irányadók. Az informatikai tárgyú szerződések általános adatvédelmi vonatkozásait nem tárgyaljuk; kizárólag azokat a csomópontokat érintjük, ahol a felhőszolgáltatás egyedi sajátosságai egyedi (vagy a szokottnál hangsúlyosabb) adatvédelmi dilemmákat vetnek fel.

2. Az Infotv. hatálya

Az Infotv. 2. § (1) bekezdése[1] a **területi hatályt** ahhoz köti, hogy az adatkezelés hol történik: az Infotv. kizárólag a *Magyarország területén* folytatott adatkezelésre és adatfeldolgozásra terjed ki. Ebből következően döntő jelentőségű kérdéssé válik, hogy – magyar illetőségű felhasználót feltételezve – pontosan hol működteti erőforrásait a szolgáltató. Ezzel azonnal a felhőszolgáltatások érzékeny pontjához értünk, hiszen globális szolgáltató esetében az erőforrások nyilvánvalóan nem, vagy legfeljebb részben magyarországi elhelyezésűek, de magyar székhelyű szolgáltatás esetében sem kizárt, hogy pl. a szolgáltatásba bevont szerverek külföldön találhatók. Nem könnyű tehát azt az alapvető kérdést sem tisztázni, hogy az Infotv. területi hatálya kiterjed-e egyáltalán az adott adatkezelésre, különös tekintettel arra, hogy a gyakorlatban az adatkezelés helyszínét jellemzően a szolgáltatóra tartozó üzemeltetési kérdésnek tekintik.
Nem egyszerűsíti a helyzetet, hogy az adatkezelés helyszíne még akkor sem feltétlenül magyarországi, ha Magyarország területén is rendelkezésre állnak a szükséges erőforrások, de más államokban ugyancsak képes ezeket biztosítani a szolgáltató.
A területi hatály problémája tehát csak úgy volna feloldható, ha a felhőszolgáltatásra kötött szerződések kötelező (de legalább ajánlott) tartalmi eleme lenne az adatkezelés (adatfeldolgozás) helyszíne.

A területi hatályhoz kapcsolódó kérdést vet még fel a külföldre történő adattovábbítás, amelyen *„az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele”* értendő. Főszabályként az Infotv. hatálya alá tartozó adatkezelő csak akkor továbbíthat személyes adatot külföldi adatkezelő részére, ha ahhoz az érintett hozzájárult, vagy biztosított az Infotv. alapvető feltételeinek megtartása és az Infotv-ben körülírt adatvédelmi szint. Fontos ugyanakkor, hogy a 5. § (4) bekezdése szerint: *„Az EGT-államba[2] irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.”* Ez utóbbi rendelkezésből következően nem szükséges sem külön hozzájárulás, sem külön

[1] **2. §** (1) E törvény hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.

[2] EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával

vizsgálat az adatvédelmi szintet illetően akkor, ha az adatkezelő olyan felhőszolgáltató részére továbbít adatot, amely ugyan külföldi, de EGT illetőségű. Így nincs törvényi akadálya (sem az általánosnál szigorúbb feltételrendszere) annak, ha a magyar adatkezelő EGT illetőségű felhőszolgáltató számára teszi hozzáférhetővé az adatokat. Az már másik kérdés, hogy magára az adatkezelésre melyik tagállami jogrend vonatkozik majd.

A **tárgyi hatály** kérdése egyfelől relatíve könnyen eldönthető, ugyanis a fent idézett 2. § (1) bekezdésében említett adatokra vonatkozó adatkezelést[3] és adatfeldolgozást[4] olyan széles értelemben definiálja a törvény, hogy nehéz volna olyan felhőszolgáltatást nyújtani, ami ne tartozna ebbe a körbe. Másfelől ugyanakkor azon a ponton szűkül a tárgyi hatály, ahol az érintett adatok körét határozza meg a jogalkotó: természetes személy adatai, valamint közérdekű adat vagy közérdekből nyilvános adat kezelése (feldolgozása) esik csak a törvény hatálya alá.

Nem mellőzhető ugyanakkor annak vizsgálata, hogy a felhőszolgáltatás **adatkezelésnek, vagy adatfeldolgozásnak** minősül, ugyanis előbbi az összes érintettől kifejezett hozzájárulást kívánna, míg utóbbira az érintettek adatait kezelő szervezettől (pl. banktól, munkáltatótól) megkapható a szükséges felhatalmazás.
Tipikus esetben a felhőszolgáltató nem magukkal az érintettekkel szerződik (azaz nem azokkal áll jogviszonyban, akikre az általa tárolt adatok vonatkoznak), hanem olyan szervezettel (pl. bankkal, munkáltatóval), amely már maga is adatkezelési tevékenységet végez harmadik személyek (banki ügyfelek, munkavállalók stb.) adatain. A jogviszony így nem az érintett és a felhőszolgáltató között, hanem az adatkezelő (bank, munkáltató) és a felhőszolgáltató között jön létre. Ilyen esetben pedig álláspontunk szerint a felhőszolgáltató tevékenysége szükségszerűen sokkal inkább *adatfeldolgozásnak* tekinthető (hiszen az adatkezelést a szerződő partner látja el, s többnyire csak technikai segítséget igényel), amely leegyszerűsítve az adatkezelést kísérő járulékos-technikai jellegű tevékenységeket foglal magában (esetünkben ez az informatikai háttér biztosítása).
Előfordulhat olyan eset is, amikor a felhőszolgáltatóval nem adatkezelőnek, hanem *adatfeldolgozónak* minősülő szervezet szerződik (pl. a munkáltató, mint adatkezelő egyes munkavállalói adatokat a könyvelő cégnek ad át adatfeldolgozásra, s ez a könyvelő cég, mint elsődleges adatfeldolgozó szerződik a felhőszolgáltatóval, mint további adatfeldolgozóval). 2013. július 1. napját megelőzően ez kizárt volt, ugyanis adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehetett igénybe. 2013. július 1. napjától azonban ez a – gyakorlatban mindig is létezett, de korábban jogellenes – helyzet többé nem tiltott: *„Az adatfeldolgozó az adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót."* A feltétel tehát mindössze az adatkezelő (írásbeli) hozzájárulása, amelyet célszerű már az adatkezelő-adatfeldolgozó (munkáltató-könyvelő) közötti szerződésben előre kikötni.

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

4 adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik

3. Az adatfeldolgozás és az adatkezelés jogalapja

3.1. Adatfeldolgozás

Az adatfeldolgozás jogalapja az adatkezelővel (pl. bankkal, munkáltatóval) megkötött szerződés, amelyre az Infotv. 9. § (4) bekezdése kötelezően írásbeli alakot rendel.
Az adatfeldolgozók körét illetően ugyanez a jogszabályhely annyi megkötést tartalmaz, hogy *„az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt”*. Tehát a felhőszolgáltató olyan üzleti tevékenységben nem lehet érdekelt, amely az érintett személyes adatokra valamilyen módon támaszkodik, azokat felhasználja.
Az adatkezelővel kötendő írásbeli szerződés határozza meg – természetesen a jogszabályi keretek között – az adatfeldolgozó jogait és kötelezettségeit. Előnyös a felhőszolgáltató számára az a jogszabályi rendelkezés, miszerint az adatkezelő által adott utasítások jogszerűségéért a felhőszolgáltatást megrendelő adatkezelő felel: a jogalkotó ezzel a szerződött partnerek viszonyában az adatkezelőre telepíti a felelősséget az utasítások, illetve azok végrehajtása terén.
Az adatfeldolgozó tevékenységének alapvető határait az Infotv. 9. § (3) bekezdése jelöli ki: *„Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.”* Ez a rendelkezés ismét az adatfeldolgozás technikai jellegét emeli ki, amely az adatfeldolgozó felelősségének előbbi korlátozását, illetve adatkezelőre hárítását is magyarázza.

Az adatfeldolgozó igénybe vételéről az adatkezelő köteles tájékoztatni az érintett ügyfeleket, munkavállalókat a velük adatkezelés tárgyában megkötött szerződésben.

3.2. Adatkezelés

Az adatkezelés jogalapja egyfelől lényeges lehet akkor, ha a felhőszolgáltató olyan érdemi tevékenységet folytat, amely már meghaladja az adatfeldolgozás szintjét és adatkezelésnek minősül, másfelől az sem érdektelen, hogy – még ha maga a felhőszolgáltató csak adatfeldolgozóként szerepel is az együttműködésben – a felhőszolgáltatóval szerződő partner adatkezelését mire alapítja (hiszen csak jogszerű alapokon zajló adatkezelésben vállalhat a felhőszolgáltató adatfeldolgozást).

[5]Személyes adat – néhány, itt nem részletezett kivételtől eltekintve – akkor kezelhető, ha:
1. ahhoz az érintett hozzájárult, vagy ha
2. annak kezelése kötelező.

5 5. § (1) Személyes adat akkor kezelhető, ha
a) ahhoz az érintett hozzájárul, vagy
b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).

3.2.1. Hozzájárulás az adatkezeléshez

Bár a hozzájárulás csak a személyes adatok szűkebb köre (ún. különleges adatok) esetében kell írásbeli legyen, nem kétséges, hogy a felhőszolgáltató (ha adatkezelőnek minősül) ezen a sérülékeny területen – a felhasználó és saját érdekében egyaránt – írásos hozzájárulással kell rendelkezzen. Ezt szükségszerűvé teszi egyébiránt az is, hogy a felek között gyakran semmiféle szóbeli kommunikáció nincsen, ráadásul írásbeli alak hiányában a jogszerű eljárás igazolása sem lehetséges (a hozzájárulás hiánya mellett pedig törvényi vélelem szól a 6. § (8) bekezdése[6] szerint), végül az Infotv. 6. § (4) bekezdéséből is az írásbeli hozzájárulás rögzítésének kötelezettsége olvasható ki.
Kiemelendő ugyanakkor, hogy a hozzájárulás megadása a felhasználói oldalon is adatvédelmi aktivitást feltételez, hiszen pl. ha egy cég a felhasználó, akkor saját döntése alapján nem adhat hozzájárulást ahhoz, hogy munkavállalói személyes adatait a szolgáltató kezelje, ehhez gondoskodni kell az érintettek beleegyezéséről (ha a szolgáltató csak feldolgozza az adatokat, akkor elégséges a tájékoztatás: l. 3.1. pont).
Vannak olyan esetek, amikor a szolgáltató azért kezel személyes adatokat, mert csak így tudja teljesíteni a felek közötti szerződést. Erre az esetkörre az Infotv. 6. § (4) bekezdése úgy rendelkezik, hogy a felek közötti szerződésben bizonyos adatvédelmi rendelkezéseknek kötelezően szerepelniük kell, elsősorban a felhasználó tájékoztatása, továbbá a hozzájárulás világos rögzítése végett: *„Ha a hozzájáruláson alapuló adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából – az Infotv. alapján – az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételének tényét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.”* Látható, hogy az idézett rendelkezés az „adatfeldolgozó igénybevételének tényét” külön kiemeli, mint az érintetteknek szóló tájékoztatás kötelező elemét, tehát javasolt, hogy a felhőszolgáltató, mint adatfeldolgozó, előzetesen tisztázza, szerződő partnere eleget tett-e ezen kötelezettségének.

3.2.2. Kötelező adatkezelések

A kötelező adatkezelésnek a felhőszolgáltatások tekintetében az adja jelentőségét, hogy a legszélesebb kört érintő, legnagyobb tömegben folytatott, s ekként a felhőszolgáltatások majdhogynem korlátlan és mindemellett rugalmasan alakítható kapacitását talán leginkább az a szféra igényelné, amely az adatkezelést jogszabályi kötelezettsége alapján folytatja.

Ugyanakkor a kötelező adatkezelést végzők kezét köti meg leginkább a jogalkotó. Az Infotv. 5. § (4) bekezdése a legérzékenyebb adatkezelési területek egyikét kifejezetten állami-önkormányzati kézben kívánja tartani: *„Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.”*
A fenti megfogalmazás aligha értelmezhető másként, mint a külső adatkezelési szolgáltatás kizárásaként, azaz ez olyan – nagyon jelentős, de nagyon szoros felügyeletet igénylő –

6 6. § (8) Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

adatkezelési tevékenység, amelyben felhőszolgáltatónak – adatkezelőként – a jelenlegi szabályozás szerint nincs helye.
Arról, hogy a felhőszolgáltató csupán adatfeldolgozóként vállalhatna-e kifejezetten technikai kisegítő szerepet ezen a területen, nem rendelkezik a törvény, de ennyire kritikus adatok tekintetében ez kifejezett jogszabályi felhatalmazás hiányában aligha lehetséges.

3.2.2.1. Kötelező adatkezelés az Eht. alapján

Kötelező adatkezelésről egyéb jogszabályok is rendelkeznek, tárgyára tekintettel talán az *elektronikus hírközlésről szóló 2003. évi C. törvény* (a továbbiakban: **Eht.**) érdemel elsőként kiemelést, hiszen ez a törvény részben éppen azt a szegmenst szabályozza, amelyen a lehetséges felhőszolgáltatók némelyike is működik.
Az Eht. a kötelező adatkezelés alanyaként az elektronikus hírközlési szolgáltatót jelöli meg. Az Infotv. 5. § (3) bekezdése[7] alapján ez úgy értelmezhető, hogy más ezeket az adatokat nem is kezelheti. Ha ez az értelmezés helyes, akkor kijelenthető, hogy a hírközlési szolgáltatók szintén nem vehetnek igénybe felhőszolgáltatást ezen adatok *kezelése* céljából.
Egyes rendelkezésekből ugyanakkor az olvasható ki, hogy *adatfeldolgozás* érdekében igénybe vehető külső szolgáltató, így akár felhőszolgáltató is.
Éppen a legsúlyosabb adatvédelmi kérdéseket felvető területen (bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzés) tartalmaz kifejezett felhatalmazást erre az Eht. 159/A. § (5) bekezdése, természetesen hangsúlyozva a garanciális feltételek teljesítésének fontosságát, így egyebek mellett azt, hogy az adatfeldolgozó EGT tagállambeli kell legyen, s ugyanígy az adattárolás sem valósulhat meg EGT tagállamon kívül: *„Az (1) bekezdés alapján adatmegőrzésre kötelezett elektronikus hírközlési szolgáltató az adatmegőrzés feladatával kizárólag abban az esetben bízhat meg adatfeldolgozóként más vállalkozást, illetve a megőrzött adatokat kizárólag abban az esetben tárolhatja az Európai Gazdasági Térség más tagállamában, ha a megőrzött adatokhoz való hozzáférés tekintetében az adatfeldolgozóval kötött adatmegőrzési szerződés tartalmazza az (1)-(2) bekezdés szerinti adatkérésekre vonatkozó hazai titokvédelmi, minősítettadat-védelmi szabályoknak megfelelő biztonsági és hozzáférési követelményeket. Az elektronikus hírközlési szolgáltató a megőrzött adatokat nem tárolhatja olyan ország területén, illetve az adatmegőrzés feladatával nem bízhat meg olyan országbeli adatfeldolgozót, amely ország az Európai Gazdasági Térségnek nem tagállama.”*

3.2.2.2. Kötelező adatkezelés az Hpt. alapján

E tekintetben világosabb és nyitottabbnak tűnő szabályozást tartalmaz *a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény* (a továbbiakban: **Hpt.**). Míg az Eht. esetében kérdéses, hogy a jogalkotó számolt-e egyáltalán a külső (azaz az elektronikus hírközlési szolgáltatókon kívüli) szolgáltatók adatkezelésének lehetőségével, s a külső adatfeldolgozó igénybevételének lehetősége is csak egy-egy rendelkezésből következik, addig a Hpt. mind a külső adatkezelés, mind a külső adatfeldolgozás lehetőségét kifejezetten tartalmazza, mégpedig 13/A és/B. §-okban.
A Hpt. a „kiszervezés” fogalmával jelöli meg a felhőszolgáltatások szempontjából releváns jogintézményt. Maga a gyakorlati szóhasználat is gyakran a „kiszervezés”-ben határozza meg a felhőszolgáltatás egyik lényegi aspektusát, ugyanis egy sokrétű felhőszolgáltatás valóban a

[7] Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

felhasználó cég informatikai tevékenységének átadását jelentheti, azzal azonban, hogy a saját informatikai tevékenység ezzel semmiképp sem szűnhet meg, inkább az egyes feladatok rangsora változhat. Visszatérve a jogszabályi fogalomra, a Hpt. a kiszervezést a következőképp határozza meg:

„a) hitelintézet esetén ha a hitelintézet a pénzügyi, illetőleg kiegészítő pénzügyi szolgáltatási tevékenységéhez kapcsolódó, illetőleg jogszabály által végezni rendelt olyan tevékenységét, amelynek során adatkezelés, adatfeldolgozás vagy adattárolás valósul meg, nem önállóan végzi, hanem annak folyamatos vagy rendszeres elvégzésére tőle szervezetileg független személlyel vagy jogi személyiséggel nem rendelkező gazdasági társasággal kizárólagos szerződést köt;

b) pénzforgalmi intézmény esetén olyan megállapodás egy pénzforgalmi intézmény és egy személy között, amelynek keretében e személy olyan pénzforgalmi szolgáltatás nyújtásának működtetéséhez kapcsolódó tevékenységet végez, amelyet egyébként a pénzforgalmi intézmény maga végezne;

c) elektronikuspénz-kibocsátó intézmény esetén olyan megállapodás egy elektronikuspénz-kibocsátó intézmény és egy személy között, amelynek keretében e személy olyan elektronikuspénz-kibocsátási vagy visszaváltási szolgáltatás nyújtásának vagy pénzforgalmi szolgáltatás nyújtásának működtetéséhez kapcsolódó tevékenységet végez, amelyet egyébként az elektronikuspénz-kibocsátó intézmény maga végezne.”

A felhőszolgáltatásra tipikusan vonatkoztatható esetet az a) pont tartalmazza, hiszen e szolgáltatás jellegzetes, sőt elengedhetetlen tartalmi eleme az a) pontban írt „*adatkezelés, adatfeldolgozás vagy adattárolás”*. Különös, hogy míg az Infotv. és az Eht. élesen megkülönbözteti az adatkezelést és az adatfeldolgozást, addig a Hpt. ezeket némiképp összemossa, sőt az „adattárolás”-t a másik két gyűjtőfogalom mellé emeli, noha az Infotv. alapján az csupán az adatkezelés egyik neme. Figyelmet érdemel továbbá a definíció utolsó fordulata, amely *„kizárólagos”* szerződés megkötéséről beszél, azaz a jogszerű kiszervezés fogalmi eleme, hogy a hitelintézet az adott szolgáltatóval olyan megállapodást kell kössön, amely kizárólagosságot biztosít. Ez a kizárólagosság azonban nem jelenti azt, hogy egyazon felhőszolgáltató ne szerződhetne több hitelintézettel, ugyanis a 13/A. § (9) bekezdése kifejezetten elismeri ennek lehetőségét, csak garanciákat ír elő e vonatkozásban: *„Az a kiszervezett tevékenységet végző, amely egyidejűleg több hitelintézet részére végez kiszervezett tevékenységet, köteles az így tudomására jutott tényt, adatot, információt elkülönítetten - az adatvédelmi előírások betartásával - kezelni.”*

A kizárólagosságon túli egyéb követelményeket már a 13/A. §[8] tartalmazza, amely a hitelintézet számára bejelentési kötelezettséget ír elő a Pénzügyi Szervezetek Állami Felügyelete (a továbbiakban: PSZÁF) felé, s ezen túlmenően igen részletesen írja körül a kiszervezés tárgyában kötendő szerződés kötelező tartalmi elemeit (lásd a 6. fejezetben).

A hitelintézetek és felhőszolgáltatók együttműködését természetesen igazán problematikussá az teszi, hogy a kezelendő vagy feldolgozandó adatok (legalábbis jelentős részben) banktitoknak[9] minősülnek. Ennek megfelelően a Hpt. csak igen szűk, taxatíve felsorolt esetekben teszi lehetővé a banktitkok kiadását. Ugyanakkor e körben is kifejezetten utalást tesz arra a törvény, hogy a tárgyalt informatikai kiszervezést a banktitkok szigorú védelme sem zárja ki, ugyanis a következőképpen rendelkezik (54. § (1) bekezdés j) pont): *Nem jelenti a banktitok sérelmét […] a hitelintézet által kiszervezett tevékenység végzéséhez szükséges adatátadás a kiszervezett tevékenységet végző részére"*.

Maga a PSZÁF is foglalkozott már a fenti kérdéskörrel 4/2012. számú Vezetői körlevelében[10], amelyben egyrészt kimondja, hogy a felhőszolgáltatás igénybevétele *„kiszervezésként kezelendő"*, másrészt összefoglalja azokat a szempontokat, amelyek ilyen

8 13/A. § (1) A hitelintézet pénzügyi-, illetőleg kiegészítő pénzügyi szolgáltatási tevékenységéhez kapcsolódó, illetve jogszabály által végezni rendelt olyan tevékenységét, amelynek során adatkezelés, adatfeldolgozás vagy adattárolás valósul meg, az adatvédelmi előírások betartása mellett kiszervezheti.
(2) A kiszervezett tevékenységet végzőnek - a kockázattal arányos mértékben - rendelkeznie kell mindazon személyi, tárgyi és biztonsági feltételekkel, melyeket jogszabály a kiszervezett tevékenységet illetően a hitelintézetre vonatkozóan előír.
(3) A hitelintézet köteles a Felügyeletnek a kiszervezésről szóló szerződés aláírását követően két napon belül bejelenteni:
a) a kiszervezés tényét, b) a kiszervezett tevékenységet végző nevét, székhelyét vagy állandó lakcímét,c) a kiszervezés időtartamát.
(4) A kiszervezésre vonatkozó szerződésnek tartalmaznia kell:
a) az adatvédelemre vonatkozó előírások érvényesülésének bemutatását, b) a kiszervezett tevékenységet végző hozzájárulását a kiszervezett tevékenységnek a hitelintézet belső ellenőrzése, külső könyvvizsgálója, az MNB és a Felügyelet helyszíni, illetve helyszínen kívüli ellenőrzéséhez, c) a kiszervezett tevékenységet végző felelősségét a tevékenység megfelelő színvonalon történő végzéséért, illetve a szerződés hitelintézet részéről történő azonnali felmondási lehetőségét a szerződés ismételt vagy súlyos megsértése esetére, d) a kiszervezett tevékenységet végzőtől elvárt, a tevékenység végzésének minőségére vonatkozó részletes követelményeket, e) a kiszervezett tevékenységet végző részéről a bennfentes kereskedelem elkerülése érdekében alkalmazandó szabályokat.
(5) A hitelintézetnek rendelkeznie kell a kiszervezésre vonatkozó szerződésben foglaltaktól történő eltérő tevékenységvégzésből eredő, rendkívüli helyzetek kezelésére kidolgozott intézkedési tervvel.
(6) A hitelintézet belső ellenőrzése köteles a kiszervezett tevékenység szerződésben foglaltaknak megfelelő végzését legalább évente megvizsgálni.
(7) A hitelintézet felelős azért, hogy a kiszervezett tevékenységet végző a tevékenységet a jogszabályi előírások betartásával és a tőle elvárható gondossággal végezze. A hitelintézetnek haladéktalanul jelentenie kell a Felügyelet részére, amennyiben a kiszervezett tevékenység végzése jogszabályba vagy a szerződésbe ütközik.
(8) A Felügyelet a hitelintézet (7) bekezdésben foglalt bejelentése vagy a helyszíni ellenőrzése során feltárt hiányosságok alapján a tevékenység kiszervezését megtilthatja.
(9) Az a kiszervezett tevékenységet végző, amely egyidejűleg több hitelintézet részére végez kiszervezett tevékenységet, köteles az így tudomására jutott tényt, adatot, információt elkülönítetten - az adatvédelmi előírások betartásával - kezelni.
(10) A kiszervezett tevékenységet végző közreműködőt abban az esetben alkalmazhat, ha a közöttük létrejövő szerződés - melyet a hitelintézetnek jóvá kell hagynia - biztosítja a kiszervezett tevékenységnek a Felügyelet, az MNB és a hitelintézet belső ellenőrzése, könyvvizsgálója által történő ellenőrzését.
(11) A hitelintézet vezető tisztségviselője vagy annak közeli hozzátartozója nem állhat tulajdonosi viszonyban a kiszervezett tevékenységet végzővel, illetve a hitelintézet vezető tisztségviselője, közeli hozzátartozója a kiszervezett tevékenység végzésével nem bízható meg.
(12) A hitelintézet a kiszervezett tevékenységek körét, és a kiszervezett tevékenység végzőjét az üzletszabályzatban köteles feltüntetni.
(13) Pénzügyi vállalkozás a Felügyelethez történő bejelentés nélkül szervezheti ki ügyviteli tevékenységét, ha azonban a kiszervezni kívánt ügyviteli tevékenység banktitkot is érint, akkor az (1)-(12) bekezdésben foglaltakat megfelelően alkalmazni kell.

9 50. § (1) Banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

10 4/2012. számú Vezetői körlevél a pénzügyi szervezeteknél a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról; 2012. július 18.

jellegű kiszervezés esetén nem hagyhatók figyelmen kívül. A körlevél nem a privát-, hanem a publikus (és ún. közösségi) felhőszolgáltatásokra összpontosít, jelezve azok nemzetközi adatvédelmi összefüggéseit is.

3.2.2.3. Egészségügyi adatok kezelése

Az egyik legnagyobb volumenű és érzékenységénél fogva leginkább védelemre szoruló adatkezelési területet az egészségügyi adatok képezik, ez indokolja, hogy röviden áttekintsük a vonatkozó szabályozást.
Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény rendkívül pontosan szabályozza az adatkezelők lehetséges körét s az adatkezelések célját. Nem rendelkezik azonban olyan egyértelműséggel az adatkezelés kiszervezése tárgyában, mint a Hpt. A kiszervezés fogalmát egyáltalán nem ismeri, s az adatkezelő definíciójában[11] nem enged helyet külső szolgáltatónak. A 34. § (1) bekezdés ugyanakkor úgy szól, hogy *„Nem egészségügyi intézmény esetén - a betegellátón kívül - adatkezelő az intézményvezető által adatkezeléssel megbízott […]személy lehet”* - ami viszont úgy értelmezhető, hogy ha *nem* egészségügyi intézmény kezel egészségügyi adatokat (erre maga a törvény is számos példát felsorol), akkor annak vezetője akár felhőszolgáltatót is igénybe vehet e célból. Ugyanakkor mindebből az is kiolvasható, hogy egészségügyi intézmény adatkezelés tárgyában efféle kiszervezési szerződést nem köthet, hiszen a törvény semmiféle, a Hpt-hez hasonló felhatalmazást erre nem ad.
Az adatfeldolgozás kiszervezhetőségét illetően a törvény érdemben nem igazít el. Szemben az adatkezelők taxatív felsorolásával, az adatfeldolgozók körét még példálózó jelleggel sem adja meg, s e tekintetben általános jellegű szabályozást sem tartalmaz.

4. Adatbiztonság

Nem vitás, hogy a felhőszolgáltatások legkritikusabb pontja az adatbiztonság. A felhőszolgáltatással szembeni bizalmatlanságot e tekintetben elsősorban az táplálja, hogy az adatkezelés a felhasználótól független, távoli eszközökön, a felhasználó számára teljeskörűen nem ismert és nem (vagy csak nehezen) ellenőrizhető módon történik.
Az adatbiztonság alapvető követelményeit az Infotv. 7. §-a[12] tartalmazza, értelemszerűen általánosságban meghatározva az adatkezelővel, illetve adatfeldolgozóval (így a

11 adatkezelő: a betegellátó; az intézményvezető; az adatvédelmi felelős; a betegjogi képviselőket foglalkoztató szerv; az egészségügyi dokumentációt kezelő szerv; továbbá közegészségügyi-járványügyi közérdekből az 5. § (3) bekezdésében meghatározott szervek és személyek; továbbá a 22. § szerinti esetekben az ott meghatározottak szerint az egészségbiztosítási szerv; a 22/E. §-ban meghatározottak szerint az orvosszakértői, rehabilitációs, illetve szociális szakértői szerv, rehabilitációs hatóság, az igazságügyi szakértői tevékenységről szóló törvény szerinti szakértő (a továbbiakban: igazságügyi szakértő); a Nyugdíj-biztosítási Alap kezeléséért felelős nyugdíj-biztosítási szerv és a nyugdíj-biztosítási igazgatási szerv; továbbá a 16/A. §-ban meghatározottak szerint, valamint a lakossági célzott szűrővizsgálatok szervezése érdekében a 3. § b) pont szerinti személyazonosító adat tekintetében az egészségügyi államigazgatási szerv; a 14/A. §-ban meghatározott adatok tekintetében a gyógyszer, gyógyászati segédeszköz, gyógyászati ellátás kiszolgáltatója, illetve nyújtója; a 15/A. §-ban meghatározottak szerint a munkavédelmi hatóság és a munkahigiénés és foglalkozás-egészségügyi szerv; továbbá a 23. § (1) bekezdés f) pontjában meghatározott esetben az első- és másodfokú etikai eljárást lefolytató kamarai szerv

12 7. § (1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

(4) 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.

(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja

felhőszolgáltatóval) szemben támasztott minimális elvárásokat, köztük kifejezetten utalva arra, hogy *„tekintettel kell lenni a technika mindenkori fejlettségére”*.
Mivel a felhőszolgáltatások gyorsabb és szélesebb körű elterjedését – különösen Európában – éppen a felhasználók adatbiztonsággal kapcsolatos félelmei hátráltatják, a felhőszolgáltatók saját (üzleti) érdeke, hogy egyfelől a lehető legmagasabb szakmai színvonalon gondoskodjanak e követelmények biztosításáról, másfelől, hogy létezzen egy olyan – a felhasználók bizalmát élvező – minősítő rendszer, amely lehetővé teszi az egyes szolgáltatók adatbiztonsági szempontú osztályozását. Ha e minősítő rendszer elméletileg kellően megalapozott és hitelesnek fogadja el a piac, akkor minden olyan területen, amelyen nem kizárt a külső szolgáltatók általi adatkezelés és adatfeldolgozás, megjelenhetnek az adott területen a felhőszolgáltatóktól elvárt egységes minőségi előírások, s az azokat igazoltan teljesítő szolgáltatók tényleges alternatívát jelenthetnek a belső erőforrásokra épülő adatkezeléssel szemben. Jelenleg a már idézett PSZÁF Vezetői körlevél hosszasan kell taglalja a megfontolásra érdemes szempontokat; ellenben, ha feláll az új minőségi osztályozási rendszer, akkor e szempontok a rendszerbe beépülnek, s az újabb körlevél már elsősorban csak az adott adatfajtához elvárt adatbiztonsági minőséget kell meghatározza. Felhasználói oldalon tehát a kiválasztási mechanizmus egyszerűsödik, a döntéshozók felelősségét részben átveszi maga a minőségbiztosítási rendszer, s az így könnyebben létrejövő felhőszolgáltatási jogviszonyok tapasztalata gyakorlatilag is megalapozhatja az egyelőre inkább csak megelőlegezett bizalmat.

5. Felek közötti együttműködés

Ahogyan már érintettük, a felhőszolgáltatás sajátosságaiból következően növekszik a szolgáltató és felhasználó közötti távolság, technikai (külső erőforrás) és kommunikációs (közvetlen kapcsolat hiánya) értelemben egyaránt. Ez a jelenség megnehezíti számos felhasználói jogosultság hatékony érvényesítését, amelyek az adatkezelés, adatfeldolgozás folyamatos kontrollját, a felhasználó viszonylagosan kiszolgáltatott adatvédelmi pozíciójának erősítését vannak hivatva biztosítani. A felhőszolgáltatók oldalán tehát tudatosítani kell, hogy a szolgáltatásra kötött szerződéssel, majd annak gyakorlati teljesítése során figyelemmel kell lenniük a kölcsönös együttműködést feltételező felhasználói jogok tiszteletben tartására, melyek közül néhányat az alábbiakban emelünk ki, azzal azonban, hogy az 5.1. pont szerinti előzetes tájékoztatást a felhőszolgáltató csak abban a – nem tipikus – esetben kell adjon, ha adatkezelést (és nem adatfeldolgozást) végez.

---

a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.
(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

5.1 Előzetes tájékoztatás

Az Infotv. 20. § (2) bekezdése szerint: *„Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.”*

Az adatkezelés célja és jogalapja a felhőszolgáltatók esetében a felhasználói oldal számára többnyire magától értetődik, hiszen célja a felek közötti szerződés teljesítése (ennek részleteit maga a felhasználó is ismeri), jogalapja pedig maga a felhasználói hozzájárulás (amely természetesen beépítendő a szerződés szövegébe). A többi említett kérdés azonban már korántsem elhanyagolható, hiszen erre a szolgáltatónak feltehetően van már bejáratott gyakorlata, de azt a felhasználó nem ismeri, legfeljebb sejti, míg nem adnak tételest tájékoztatást róla.

A nagy ügyfélkörrel rendelkező felhőszolgáltatókra előnyös könnyítést tartalmaz a 20. § (4) bekezdés, amely arra az esetre, ha *„az érintettek személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna”* az egyedi tájékoztatás helyett csupán bizonyos információk[13] nyilvánosságra hozatalát írja elő.

5.2. Tájékoztatás, helyesbítés, törlés

Akár adatkezelést, akár adatfeldolgozást végez a felhőszolgáltató, elengedhetetlen a felhasználói jognyilatkozatok folyamatos fogadásának és kezelésének megfelelő megoldása a szerződés fennállása idején is. A felhasználó ugyanis az adatkezelőtől bármikor kérhet személyes adatainak kezelésével kapcsolatos tájékoztatást, helyesbítést, vagy valamely adat törlését, s ezt a felhőszolgáltatónak kell végrehajtania akkor is, ha csak adatfeldolgozóként jár el.
A tájékoztatás annyiban érdemel figyelmet, hogy ha a szolgáltató adatot továbbítana, akkor ún. adattovábbítási nyilvántartást köteles vezetni.
A törlés már kritikusabb kérdés, hiszen valamely személyes adat tárolása éppúgy sértheti a felhasználó érdekét, mint elvesztése, megsemmisülése. Gondoljunk csak arra az egyszerű esetre, amikor a felhőszolgáltatóval létrejött szerződés megszűnik, s akár egy nagyvállalat több évre visszamenőlegesen rendelkezésre álló, üzleti titkokat és egyéb érzékeny információit tartalmazó adatállományát kell törölni. A törlés kapcsán az a legfontosabb követelmény, hogy a szolgáltató olyan rendszert működtessen, amelyben a törléssel az adat technikai értelemben is véglegesen és helyreállíthatatlanul megsemmisül. Informatikai adatok esetén ez megfelelően biztonságos eljárás (többszörös véletlenszerű felülírás) alkalmazását tételezi fel. A felhőszolgáltatók minősítése tekintetében a törlési kérelem gyors és megbízható teljesítése feltétlenül szempont kell legyen.

13 a) az adatgyűjtés ténye,
b) az érintettek köre,
c) az adatgyűjtés célja,
d) az adatkezelés időtartama,
e) az adatok megismerésére jogosult lehetséges adatkezelők személye,
f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése, valamint
g) ha az adatkezelés adatvédelmi nyilvántartásba vételének van helye, az adatkezelés nyilvántartási száma, kivéve a 68. § (2) bekezdésében foglalt esetet.

5.3. Adatvédelmi felelős

Az Infotv. 24. § (1) bekezdése – lényegében az adatvédelmi előírások érvényesülésének biztosítékaként – adatvédelmi felelős megbízását írja elő néhány adatkezelő és adatfeldolgozó számára. Ilyen többek között a pénzügyi szervezet, vagy az elektronikus hírközlési szolgáltató is. Mivel előbbi esetében a Hpt. kifejezetten lehetővé teszi – kiszervezés keretében – adatkezelő vagy adatfeldolgozó felhőszolgáltató igénybevételét, felmerülhet, hogy az e lehetőséggel élő pénzügyi intézménynél ugyan működik adatvédelmi felelős, de az adatkezelés (adatfeldolgozás) javát ellátó szolgáltatónál nem. Ezt a visszás helyzetet kerüli el akkor a Hpt, amikor a 13/A. § (2) bekezdésében előírja: *„A kiszervezett tevékenységet végzőnek - a kockázattal arányos mértékben - rendelkeznie kell mindazon személyi, tárgyi és biztonsági feltételekkel, melyeket jogszabály a kiszervezett tevékenységet illetően a hitelintézetre vonatkozóan előír."* Bár e rendelkezés lehetővé teszi a mérlegelést („kockázattal arányos mérték"), így az értelmezési viták lehetőségét sem zárja ki, de ennek alapján aligha kerülheti el a pénzügyi intézmény szerződő felhőszolgáltató saját adatvédelmi felelős foglalkoztatását. Ez a kitétel ugyanakkor nemcsak az adatvédelmi felelős kapcsán bír jelentőséggel, hiszen arra kötelezi a felhőszolgáltatókat, hogy minden tekintetben alkalmazkodjanak a Hpt. vonatkozó feltételrendszeréhez, ha a Hpt. hatálya alá tartozó kiszervezés keretében kívánnak szerződést kötni.

6. Felhőszolgáltatásra kötött szerződés javasolt és kötelező feltételei a Hpt-re figyelemmel

Az előbbiekben részletezett elméleti megközelítés után – úgy is mint a teoretikus problémafelvetések gyakorlati próbája – indokolt röviden vázolni, milyen tartalmi elemeket vár el a jelenleg hatályos Infotv. és Hpt. attól a szerződéstől, amelyet egy Hpt. hatálya alá tartozó pénzügyi intézmény felhőszolgáltatásra kötne. Annak oka, hogy a speciális szakági jogszabályok közül konkrétan a Hpt. példáján mutatjuk be a gyakorlati alkalmazást, mindenekelőtt az, hogy egyedül ebben a törvényben találhatók szabatosan megfogalmazott kritériumok az ilyen jellegű kiszervezésekre vonatkozóan, s így csak ezen a területen tekinthetjük egyértelműnek a felhőszolgáltatási szerződések megkötésének elvi lehetőségét. Az alábbiak kizárólag akkor irányadók, ha az adatkezelés Magyarországon történik, s így a magyar pénzügyi intézmény által megbízott szolgáltatóra és a közöttük létrejött jogviszonyra a magyar jog alkalmazandó.

6.1. A szerződő felek, a szerződés tárgya

A Hpt. a felhőszolgáltatási szerződés tartalma tekintetében – nem kizárólag, de elsősorban – akkor irányadó, ha felhasználói oldalon a törvény hatálya alá tartozó szervezet szerződik, amelyet a Hpt. „pénzügyi intézménynek" nevez. A pénzügyi intézmény két fajtája a „hitelintézet" és a „pénzügyi vállalkozás". A hitelintézetek a Hpt. 3. § (1) bekezdése szerinti pénzügyi szolgáltatások[14] szélesebb körét jogosultak nyújtani, mint a pénzügyi vállalkozások,

14 Hpt. 3. § (1) Pénzügyi szolgáltatás a következő tevékenységek üzletszerű végzése forintban, illetőleg devizában, valutában:
a) betét gyűjtése és más visszafizetendő pénzeszköz - saját tőkét meghaladó mértékű - nyilvánosságtól történő elfogadása;
b) hitel és pénzkölcsön nyújtása;
c) pénzügyi lízing;
d) pénzforgalmi szolgáltatások nyújtása;
e) elektronikus pénz kibocsátása;
f) olyan papír alapú készpénz-helyettesítő fizetési eszköz (például papír alapú utazási csekk, váltó) kibocsátása, illetve az ezzel kapcsolatos szolgáltatás nyújtása, amely nem minősül pénzforgalmi szolgáltatásnak;
g) kezesség és bankgarancia vállalása, valamint egyéb bankári kötelezettség vállalása;

tehát a két intézménytípus között ez az alapvető különbség. A mindennapi életből közismert bankok és takarékszövetkezetek hitelintézetnek minősülnek. Egyedül a bankok kaphatnak engedélyt a pénzügyi szolgáltatások teljes körének végzésére, ezzel tehát bizonyos értelemben kiemelkednek a pénzügyi intézmények köréből.
Amennyiben a felhőszolgáltató bankkal szerződik, bizonyos lehet abban, hogy a jogviszony tekintetében a Hpt. rendelkezései is jelentőséggel bírnak. Ha a szerződő fél nem bank, akkor a helyzet nem ennyire egyértelmű; ilyen esetben vizsgálandó, hogy a Hpt. hatálya alá tartozó szervezet-e a felhasználó.

A felhőszolgáltatási szerződés tárgya gyakran (jellemzően) nem maga az adatkezelés, adatfeldolgozás, vagy annak minősülő valamely művelet, hanem pl. szoftverek biztosítása, üzemeltetése. Kétségtelen ugyanakkor, hogy a szolgáltatás, annak elsődleges tárgyától függetlenül, minden esetben együtt jár valamilyen, jellemzően az adatfeldolgozás körébe eső tevékenységgel. Ennek megfelelően már a tárgy megjelölésekor javasolt utalni az adatfeldolgozás (esetleges adatkezelés) alapvető körülményeire.

6.2. Előzetes adatvédelmi tájékoztatás

Adatkezelési tevékenység esetén az adatkezelés alapvető körülményeit célszerű külön mellékletbe foglalni, s annak tartalmát az Infotv. 20. § (2) bekezdéséhez igazodva – előzetes adatvédelmi tájékoztatóként – kidolgozni:
a) adatkezeléssel érintett adatok köre, osztályozása,
b) adatkezelés célja,
c) adatkezelés jogalapja,
d) adatkezelő személye,
e) adatkezelés időtartama,
f) adatokhoz (esetlegesen) hozzáférő személyek,
g) az adatkezeléssel kapcsolatos felhasználói jogok,
h) az adatkezeléssel kapcsolatos felhasználói jogorvoslati lehetőségek.

Valójában a felsorolt szempontok részletezése – értelemszerű módosításokkal – akkor is javasolt, ha a felhőszolgáltató adatfelsolgozást és nem adatkezelést vállal.

A fenti felsorolásban első helyen szereplő adatkör- és osztályozás nem elsősorban az Infotv. 20. §-ából következik, hanem abból, hogy mindkét szerződő fél számára csak akkor lehet világos a felhőszolgáltatási jogviszony adatvédelmi területének jelentősége és a megfelelő védelmi szint meghatározása, ha számba veszik, milyen személyes adatokat érint majd a szolgáltató adatkezelése (adatfeldolgozása). Osztályozáson itt – mivel pénzügyi intézmény áll felhasználói oldalon – nem elsősorban az Infotv. szerinti osztályozás értendő (hiszen ún. „különleges adat” nemigen áll a pénzügyi intézmények rendelkezésére), hanem a pénzügyi intézmények számára kiemelt fontosságú banktitok kell legyen az osztályozási szempont: a banktitok sérthetetlensége felől kell megállapítani az egyes adatfajták érzékenységét, számolva természetesen azzal is, hogy milyen fajta adatok közötti kapcsolatot kell kizárni vagy korlátozni. További osztályozási szempont – a bennfentes kereskedelem tilalmának

h) valutával, devizával - ide nem értve a pénzváltási tevékenységet -, váltóval, illetve csekkel saját számlára vagy bizományosként történő kereskedelmi tevékenység;
i) pénzügyi szolgáltatás közvetítése;
j) letéti szolgáltatás, széfszolgáltatás;
k) hitel referencia szolgáltatás.

Tőkepiaci tv. szerinti szabályozására tekintettel – az ún. bennfentes információk elkülönítése (bővebben a 6.4. f) pontban).
Az adatkezelés (adatfelsdolgozás) célja a szerződés fő tárgyára figyelemmel, ahhoz képest írható körül legegyszerűbben, az adatkezelés (adatkezelés) jogalapja pedig maga a szerződésbe foglalt felhasználói nyilatkozat a szerződés szerinti adatkezeléshez való kifejezett hozzájárulásról (illetve adatfeldolgozásra szóló megbízásról).
Az adatkezelő személye a felhőszolgáltatóval kell azonos legyen, ellenkező esetben maga a felhasználói hozzájárulás, és a szerződés egyéb adatvédelmi vonatkozásai is értelmezési gondokat vetnének fel, kezdve attól, hogy van-e egyáltalán tényleges és jogszerű jogalapja bármilyen adatkezelésnek.
Az adatkezelés (adatfeldolgozás) időtartama szorosan összefügg a szerződés időtartamával, de nem feltétlenül azonos azzal. Ennek kapcsán mindenekelőtt arról kell dönteni, hogy a szerződés megszűnése esetén mi volna a pénzügyi intézmény elvárása (az adatok teljeskörű törlése, vagy egyéb), ehhez kell-e külön jognyilatkozatot tennie a pénzügyi intézménynek (pl. adattörlési kérelem), illetve ha az adatkezelés nem szűnik meg a szerződés megszűnésekor, akkor mely szerződéses (elsősorban adatkezelésre vonatkozó) rendelkezések maradnak hatályban stb. Annak is lehet jelentősége az adatkezelés időtartama tekintetében, hogy a szerződés megszűnésének mi az oka (ha a határozott idő lejárta, akkor előre tervezhető a külső erőforrásokon kezelt adatok sorsa, ellenben pl. a pénzügyi intézmény azonnali hatályú felmondása esetén magának a pénzügyi intézménynek okozhat gondot, ha automatikusan töröl mindent a szolgáltató).
Azt, hogy kik ismerhetik meg a kezelt (feldolgozott) adatokat, a felhőszolgáltató felelőssége pontosan és teljeskörűen megadni, figyelemmel arra is, hogy a szerződés fennállása alatt ez változhat. E vonatkozásban nyilvánvalóan a felhőszolgáltató minősített védelmi szintje alapozhatja meg a bizalmat.
Az adatkezeléssel kapcsolatos felhasználói jogok (tájékoztatás, helyesbítés, törlés, zárolás, kártérítés) tekintetében az Infotv. 14-18. és 23. §§-ainak beemelése látszik célszerűnek, a jogorvoslati lehetőségeket (tiltakozás, bírói út) illetően pedig a 21-22. §§-ok rögzítése.

Külön figyelmet érdemel az adatkezelő kártérítési felelősségének szabályozása, ugyanis végső soron ez az igazi és legsúlyosabb polgári jogi szankciója a felhőszolgáltató esetleges szerződésszegésének, így a szerződésszerű adatkezelés egyik legfőbb biztosítéka is.
Az Infotv. 23. § (1) bekezdés első mondata így szól: *„Az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt köteles megtéríteni.”*
Az adatkezelés jogellenessége kevésbé merül fel, hiszen magán a szerződésen alapul, de a második fordulatban említett *„adatbiztonság követelményeinek megszegése”* már nagyon is gyakorlati jelentőségű: ha egy pénzügyi intézmény szerződésszegéstől tart, akkor alapvetően ettől tart, s ebből valóban komoly kárai származhatnak.
Az adatkezelő kártérítési felelőssége objektív, tehát a felhőszolgáltató nem mentheti ki magát azzal (mint a Ptk. általános kártérítési felelőssége esetében), hogy „úgy járt el, ahogyan az adott helyzetben általában elvárható”. Abszolút kimentési oknak kizárólag a vis maior minősül (*„Az adatkezelő mentesül a felelősség alól, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő”*), továbbá – relatív kimentési okként – a felhőszolgáltatónak nem kell megtérítenie a kárt *„annyiban, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott”*. Megjegyzendő, hogy a „szándékosság” és „gondatlanság” fogalmait csak a büntetőjogi joganyag és joggyakorlat dolgozta ki egyértelműen és alaposan; a polgári jog területén ezek a kategóriák igen ritkán használatosak és – talán épp ezért – nehezen értelmezhetőek.

Az adatkezelés tehát a kárfelelősség tekintetében egyfajta „veszélyes üzem”, s ha megállapítható az adatbiztonsági követelmények megsértése, s az ezzel okozati összefüggésben bekövetkezett kár, akkor a felhőszolgáltató kártérítés fizetésére köteles. Ebből a kárfelelősségi szabályozásból a pénzügyi intézmény nem engedhet, már csak azért sem, mert ő maga is adatkezelő az ügyfelekkel szemben, s e pozíciójában ő maga is ilyen felelősséget visel.
Amennyiben a felhőszolgáltató nem adatkezelőnek, csupán adatfeldolgozónak minősül, úgy közvetlenül az érintett felé nem felel: *„Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért is.”* Ez azonban csupán annyit jelent, hogy az adatfeldolgozó nem az érintett felé, hanem az adatkezelő felé tartozik felelősséggel, azaz egymás közötti viszonyukban az adatkezelő értelemszerűen áthárítja az adatfeldolgozó által okozott kárt.
Olyan piacon, ahol globális szolgáltatók működnek – és a felhőszolgáltatás tipikusan ilyen – jellemző a külföldi (különösen angolszász) jogintézmények, feltételrendszerek beszivárgása a szerződésekbe, még magyar illetőségű felek esetén is. A kártérítési felelősség korlátozása pedig különösen „divatos” jelenség ezekben a nemzetközi mintákat követő megállapodásokban, amelyekkel vélhetően a legtöbb felhőszolgáltató ajánlatként előáll. Ezért nagyon lényeges, hogy akárkivel is szerződik a pénzügyi intézmény, a kártérítési klauzula az Infotv. előbb elemzett rendelkezéseihez igazodjon, mindenfajta megszorítás, korlátozás nélkül.

Az Infotv. 20. § (2) bekezdése ugyan nem nevesíti, de feltétlenül javasolt az adatkezelés (adatfeldolgozás) helyének rögzítése is, amely Magyarország területén kell történjen, ellenkező esetben a tevékenység kikerül az Infotv. – és ezzel az alapvető magyar adatvédelmi szabályozás – területi hatálya alól. Nincsen szó természetesen jogsértésről akkor sem, ha a szerződés adatkezelés helyeként külföldi helyszínt ad meg, ezesetben azonban a magyar jogrend aligha alkalmazható.

6.3. Megbízás az adatfeldolgozásra, hozzájárulás az adatkezeléshez,

Az adatfeldolgozás jogalapja az adatkezelő megbízása, az adatkezelés elsődleges jogalapja pedig, ahogyan már említésre került, maga az érintettől származó hozzájárulás, amely jelentősége miatt külön szerződéses rögzítést érdemel. A megbízás, illtve hozzájárulás egyszerre kell teljeskörű és pontos legyen, ami akkor oldható meg, ha meghivatkozható a 6.2. pont szerinti melléklet (előzetes adatvédelmi tájékoztató), amelynek gyakorlati haszna egyebek mellett éppen a megbízás, hozzájárulás szabatos megfogalmazhatóságában áll.

6.4. A Hpt. ált előírt szerződéses feltételek

A Hpt. már idézett rendelkezési kötelező tartalmi elemként az alábbi tárgyakat jelölik meg:

a) az adatvédelemre vonatkozó előírások érvényesülésének bemutatása,
b) a kiszervezett tevékenységet végző hozzájárulása a kiszervezett tevékenységnek a hitelintézet belső ellenőrzése, külső könyvvizsgálója, az MNB és a Felügyelet (PSZÁF) helyszíni, illetve helyszínen kívüli ellenőrzéséhez,
c) a kiszervezett tevékenységet végző felelősségvállalása a tevékenység megfelelő színvonalon történő végzéséért,
d) a szerződés hitelintézet részéről történő azonnali felmondási lehetősége a szerződés ismételt vagy súlyos megsértése esetére,

e) a kiszervezett tevékenységet végzőtől elvárt, a tevékenység végzésének minőségére vonatkozó részletes követelmények,
f) a kiszervezett tevékenységet végző részéről a bennfentes kereskedelem elkerülése érdekében alkalmazandó szabályok.

Az adatvédelemre vonatkozó előírások érvényesülésének bemutatása nem teljesül ugyan önmagában a 6.2. pontban részletezett adatvédelmi tájékoztatóval, de ha a szerződés a jelen 6. fejezetben javasolt egyéb adatvédelmi vonatkozásokat is tartalmazza, akkor álláspontunk szerint már megfelel e követelménynek, különösen, ha az adatvédelem érvényesülésének technikai oldala is szakszerűen bemutatásra kerül.

A b) pont szerinti hozzájárulás kifejezetten annak biztosítéka, hogy a Hpt-ben szereplő, a pénzügyi intézményekkel szemben támasztott követelmények ellenőrizhetősége, illetve az ellenőrzés hatékonysága ne szenvedjen csorbát a kiszervezés eredményeként. Különösképpen elengedhetetlen e felügyeleti szervek akadálytalan eljárása arra tekintettel, hogy a felhőszolgáltató a belső munkaszervezési folyamatok és az ügyfélérdekek szempontjából egyaránt kifejezetten érzékeny területen tevékenykedik.

A c) pontban foglalt felelősségvállalás tartalmi lényege nyilvánvalóan nem az, hogy ezt az általános megfogalmazást a szerződésbe is beemeljék. Itt jutna döntő jogi szerephez az a minőségbiztosítási rendszer, amelynek szükségességéről már a 4. fejezetben szóltunk. A szerződő felhőszolgáltatót ennek alapján minőségi osztályba sorolnák, s tevékenységének mércéje (a „megfelelő színvonal", ahogy a Hpt. fogalmaz) ettől kezdődően az általa vállalt minőségi osztály követelményszintje volna: ez tenné gyakorlatilag is igazolhatóvá, ha valamilyen tekintetben esetleg elmarad az elvárt szakmai szinttől, s ez tenné gyakorlatilag is érvényesíthetővé felelősségét.

Az azonnali felmondás lehetősége kapcsán a Hpt. viszonylagosan nagyvonalú, hiszen csak szerződésszegés esetére írja elő e lehetőséget, azaz láthatóan fontosabbnak tételezi a felhőszolgáltatási szerződések stabilitását, mint a pénzügyi intézmények „menekülési útjának" biztosítását. Ez a kritérium ugyanis egyáltalán nem zárja ki annak lehetőségét, hogy a felhőszolgáltatóval kötött szerződés a felhőszolgáltató pozícióját akár évekre biztosítsa, hiszen amíg nem követ el – súlyos vagy ismételt – szerződésszegést, addig a jogviszony egyoldalúan nem szüntethető meg, ha a felek a Hpt. minimumelvárásait követik e téren. Természetesen a Hpt. azt sem tiltja, hogy a pénzügyi intézménynek szerződésszegés hiányában is legyen lehetősége a felmondásra, de erre sem a pénzügyi intézményt, sem a másik oldalt nem kényszeríti rá. A felek tehát ebben a nagyon lényeges kérdésben szabadon állapodhatnak meg, s így az lehet majd irányadó, hogy határozott, vagy határozatlan idejű szerződést kötnek. Előbbi esetben a szerződésszegés hiányában történő felmondás általában kizárt, vagy (pl. kötbérrel) szankcionált, utóbbi – tehát határozatlan idejű szerződés – esetén viszont természetes a szerződésszegéstől független felmondási lehetőség (amely ugyanakkor nem azonnali hatályú, hanem jellemzően felmondási idővel „halasztott" felmondást jelent).
A jogviszony megszűnésének egyes eseteit[15] feltétlenül ajánlott részletesen szabályozni, több okból is.

[15] - határozott idejű szerződésben: határozott idő lejárta, egyoldalú megszüntetés lejárat előtt és után, ezen belül megkülönböztetve a szerződésszegésre alapított és annak hiányában történő felmondás lehetőségét (lejárat előtt tipikusan kizárt a szerződésszegés hiányában történő felmondás, azt követően felmondási idő mellett megengedett)
- határozatlan idejű szerződésben: jellemző a szerződésszegés hiányában történő felmondás lehetősége, megfelelően hosszú felmondási idővel

Egyrészt bármiféle komolyabb szerződéses konfliktus esetén kiemelt jelentőséget kap a szerződés megszűnésére és megszüntetésére vonatkozó szabályozás, amelyet ezért nem érdemes a háttérjogszabályok általános rendelkezéseire bízni (különösen azért sem, mert a felhőszolgáltatási szerződés egyetlen Ptk-beli szerződéstípusba sem lesz besorolható, s így nagyon nehéz megválaszolni, mely Ptk. rendelkezések tekinthetők adott esetben irányadónak).
Másrészt konokul tartja magát az a téves közvélekedés, amely szerint a szerződéseket főszabályként fel lehet mondani (egyoldalúan meg lehet szüntetni), ha a szerződés ezt nem zárja ki. A magyar polgári jogi szabályozás azonban épp fordított: a szerződést akkor lehet egyoldalúan megszüntetni (felmondás, elállás), ha arra a szerződő felet jogszabály vagy maga a szerződés kifejezetten feljogosítja[16]. Ilyen jogszabályi felhatalmazás szerepel pl. a Ptk. késedelemre, illetve szavatossági felelősségre vonatkozó szabályai között, amelyek azonban szolgáltatói késedelem, illetve hibás teljesítés (azaz: **szerződésszegés**) esetére teszi lehetővé a felmondást (elállást). Kétségtelen, hogy egyes szerződéstípusoknál, így pl. a vállalkozási szerződés esetén a Ptk. ismeri az ún. „általános" (szerződésszegés hiányában történő) elállás lehetőségét, csakhogy erre az esetre az elállással okozott kár megtérítését is előírja[17]. Így ha a felek bármelyike azt kívánja biztosítani, hogy szabadulhasson a kötelemből, még akkor is, ha nem történt szerződésszegés, erre kifejezett rendelkezéseket kell beépítenie a szerződés szövegébe, ellenkező esetben erre nem lesz módja.
Szintén célszerű a szerződésszegés azon tipikus eseteit, amelyek a gyakorlatban előfordulnak és általában súlyosnak tekinthetők, legalább példálózó jelleggel felsorolni, ennek hiányában ugyanis komoly viták forrása lehet a szerződésszegés súlyának és az erre alapított (azonnali hatályú) felmondás jogszerűségének megítélése.

Az e) pont szerinti minőségi követelmények meghatározásának egységességét és kellő részletességét a már többször emlegetett minőségi osztályba sorolás feltételrendszerének kidolgozása és általános „szakmai szabványként" való alkalmazása biztosíthatja. A c) pontban írt „megfelelő színvonal" és az e) pont minőségi követelményei tehát aligha választhatók el egymástól, s mindkettő tartalmi hátterét a minőségbiztosítási rendszer adja majd.

Az f) pontban írt bennfentes kereskedelem elkerülése kifejezetten a Hpt. alá tartozó szervezetekre szabott speciális követelmény, amely – hasonlóan a b) pont szerint elvárt közvetlen felügyelet biztosításhoz, illetve tudomásul vételéhez – nem a kiszervezés és nem is a felhőszolgáltatás sajátosságából, hanem az azt igénybe vevő felhasználó (pénzügyi intézmény) működési területének legfőbb veszélyforrásából eredeztethető.
A bennfentes kereskedelem fogalmát nem a Hpt., hanem *a tőkepiacról szóló 2001. évi CXX. törvény* (a továbbiakban: **Tőkepiaci tv.**) határozza meg. E jogszabály (leegyszerűsítve) az értékpapír-kereskedelem alapvető szabályait tartalmazza, s külön fejezetben tárgyalja a bennfentes kereskedelem (valamint az azzal „rokon" piacbefolyásolás) tilalmát. Maga a fogalommeghatározás igen bonyolult, ugyanis más, szintén önálló definiálására és értelmezésre szoruló fogalmakra épül (ezek a „bennfentes személy" és a „bennfentes információ").

[16] Ptk. 320. és 321. § (1) Aki szerződésnél vagy jogszabálynál fogva elállásra (felmondásra) jogosult, e jogát a másik félhez intézett nyilatkozattal gyakorolja.

[17] Ptk. 395. § (1) A megrendelő a szerződéstől bármikor elállhat, köteles azonban a vállalkozó kárát megtéríteni.

Anélkül, hogy a teljes fogalmi rendszert kibontanánk, röviden vázolni kell a bennfentes kereskedelem tilalmának logikáját, hogy érzékelhető legyen, mennyiben érintheti mindez a felhőszolgáltatási jogviszonyt, és magát a felhőszolgáltatót.
Az első a bennfentes személy körülírása, ugyanis ő az, aki megsértheti a tilalmat. A Hpt. hatálya alá tartozó szervezetek és a felhőszolgáltatók szempontjából a Tőkepiaci tv. 201. § (2) bekezdésének f), g) és i) pontjai lehetnek a legfontosabbak, ugyanis ezek szerint bennfentes személy:
„f) a kibocsátó számlavezető hitelintézete, illetve ennek vezető tisztségviselője, felügyelőbizottsági tagja és érdemi ügyintézője;
g) aki a bennfentes információt munka- vagy feladatköréből kifolyólag, munkavégzése vagy szokásos feladatainak elvégzése során kapta meg, vagy egyéb módon jutott tudomására;
i) az a)-h) pontban felsorolt természetes személlyel közös háztartásban élő személy, illetőleg közeli hozzátartozója."
Amint látható, maga a számlavezető hitelintézet, pusztán e szerepéből adódóan, bennfentes személynek minősül, ráadásul így sorolja be a törvény még az „érdemi ügyintéző" személyét is. Ennek alapján már világos, hogy a Hpt. miért tartja elsőrendű kérdésnek e tilalom megtartásának garantálását. Azonban nemcsak a számlavezető hitelintézet érezheti magát közvetlenül érintettnek, hanem a kiszervezett tevékenységet végző felhőszolgáltató is, hiszen a g) pont szerinti körbe feltétlenül beletartozik, ha a tudomására jutott információ „bennfentes"-nek ítélhető. Az i) pont azért érdemel figyelmet, mert szokatlan mértékben kiterjeszti a felelősök alanyi körét, s ezzel egyszersmind a tilalom súlyát is jelzi.
Ahogyan a fentiekből megállapítható, a felhőszolgáltató számára lényeges kérdés, hogy az általa kezelt (feldolgozott) adatok közül melyek tekintendők bennfentes információnak[18]. Ennek részletes elemzése meghaladná a jelen tanulmány kereteit, itt csak a tipikus bennfentes információ jellemzőit jelöljük meg: olyan lényeges információ, amely még nem került nyilvánosságra, pénzügyi eszközre (vagy annak kibocsátójára) vonatkozik és alkalmas arra, hogy a pénzügyi eszköz árfolyamát lényegesen befolyásolja.
Ami a bennfentes kereskedelem elkerülését szolgáló szabályokat illeti, e körben a Tőkepiaci tv. bizonyos (a PSZÁF, illetve a kibocsátó felé teljesítendő) bejelentési, továbbá nyilvántartás vezetési kötelezettséget ír elő. A felhőszolgáltatót sokkal inkább az utóbbi érinti, ugyanis a Tőkepiaci tv. 201/D. § (1) bekezdése szerint *„a bennfentes kereskedelemhez kapcsolódó hatósági ellenőrzés elősegítése érdekében a kibocsátó a munkaviszony vagy egyéb jogviszony alapján részére tevékenységet végző és bennfentes információhoz hozzáférő személyekről nyilvántartást vezet, amelyet a Felügyelet kérésére, a nyilvántartást vezető személy köteles átadni."* Az nem kétséges, hogy maga a pénzügyi intézmény „bennfentes információhoz

[18] 201. § (3) Bennfentes információ:
a) a pénzügyi eszközzel - ide nem értve az árualapú származtatott ügyletet - kapcsolatos olyan lényeges információ, amely
aa) még nem került nyilvánosságra;
ab) közvetlenül vagy közvetve a pénzügyi eszközre vagy a pénzügyi eszköz kibocsátójára vonatkozik;
ac) nyilvánosságra kerülése esetén a pénzügyi eszköz árfolyamának lényeges befolyásolására alkalmas;
b) a pénzügyi eszközzel kapcsolatos megbízások végrehajtásával megbízott személyek esetében olyan lényeges információ az a) pontban meghatározottakon kívül, amely az ügyfél által adott és az ügyfél folyamatban lévő megbízásához kapcsolódik;
c) az árualapú származtatott ügylettel kapcsolatos olyan lényeges információ, amely
ca) még nem került nyilvánosságra;
cb) közvetlenül vagy közvetve az árualapú származtatott ügyletre vonatkozik;
cc) az elfogadott piaci gyakorlat alapján a piaci szereplők tudomására hozandó;
cd) információt a piac szereplőivel rendszeresen közölnek.
(4) Lényeges információ: minden olyan információ, amely olyan eseményre vagy körülményre vonatkozik, amely bekövetkezett vagy bekövetkezése megalapozottan várható, és elég konkrét ahhoz, hogy lehetővé tegye következtetések levonását az adott körülménynek vagy eseménynek egy adott pénzügyi eszköz árfolyamára esetlegesen gyakorolt hatásáról.
(5) Az árfolyam befolyásolására alkalmas információ: minden olyan információ, amely a befektető által nagy valószínűséggel felhasználásra kerülne befektetési döntése meghozatalakor.

hozzáférő személy"-nek minősül, de kiterjesztő értelmezés esetén ebbe a kiszervezett tevékenységet végző felhőszolgáltató is beleértendő, azaz nyilvántartásba kell vegyék.
Összességében a bennfentes kereskedelemmel kapcsolatban megítélésünk szerint elegendő, ha a felhőszolgáltatási szerződés:

- utal – akár a Tőkepiaci tv. vonatkozó rendelkezéseinek idézetével – az előbb taglalt alapfogalmakra (bennfentes információ, bennfentes személy, bennfentes kereskedelem),
- az adott jogviszonyra konkretizálja ezeket (a felhőszolgáltató által kezelt adatok közül melyek esnek a bennfentes információ körébe, kik milyen okból és milyen terjedelemben férhetnek hozzá, e hozzáférések visszakövetése – naplózása – miként biztosított),
- kifejti, hogy érinti-e és mennyiben a felhőszolgáltatót bármiféle bejelentési, vagy a nyilvántartásba vétellel kapcsolatos kötelezettség,
- összefoglalja azokat az előírásokat, amelyek az adott pénzügyi intézménynél a bennfentes kereskedelem tilalmának érvényesülését biztosító eljárásrendet tartalmazzák (feltételezve, hogy a Hpt-re tekintettel ilyennel rendelkeznek a pénzügyi intézmények) és megjelöli, hogy ezek mennyiben terjednek ki a felhőszolgáltatóra.

6.5. Banktitok, üzleti titok, titoksértési tilalmak

A banktitok és az üzleti titok a pénzügyi intézmény és a felhőszolgáltató közötti jogviszony olyan lényeges fogalmai, amelyekre akkor is ki kell térjünk, ha maga a szerződés esetleg csak mint mindkét fél által ismert jogintézményt kezeli azokat. Nem elvárás tehát, hogy a szerződés kifejezetten részletezze e kérdést, de elvárás, hogy ne csak a felhasználói, hanem a szolgáltatói oldal is tisztában legyen azzal, mit is jelent a banktitok és az üzleti titok.
A banktitok kifejezetten a Hpt. által bevezetett fogalom: *„Banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik."*
Banktitok tehát szinte minden adat, amely az ügyfélhez köthető. Kérdés persze, hogy ki minősül ügyfélnek. A Hpt. szerint: *„E törvény banktitokra vonatkozó rendelkezései szempontjából a pénzügyi intézmény ügyfelének kell tekinteni mindenkit, aki (amely) a pénzügyi intézménytől pénzügyi szolgáltatást vesz igénybe."* A pénzügyi intézmény és pénzügyi szolgáltatás jelentését a 6.1. pontban tárgyaltuk. Ha mindezeket a meghatározásokat egymással összhangban értelmezzük, akkor megállapítható, hogy a pénzügyi intézmény ügyfelekkel fennálló kapcsolatában keletkező adatok, amelyek az ügyfélhez rendelhetők, banktitoknak tekintendők. Így ha a felhőszolgáltató ezen a területen is tevékenykedik, akkor banktitkokat kezel (dolgoz fel).
A banktitok természetesen rendkívül szűk körben adható ki, ezeket az eseteket a Hpt. 51-54. §§-ai sorolják fel tételesen.

Az üzleti titok definícióját a Ptk. tartalmazza, a Hpt. is erre utal vissza: *„Üzleti titok a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult - ide nem értve a magyar államot - jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette."* Ebből kiolvashatóan magára a pénzügyi intézményre vonatkozó adatok tartozhatnak ebbe a körbe, és természetesen ez a kategória átfedésben lehet a banktitkokkal is, ha mindkét titokfajta fogalmi elemei megvalósulnak. A

Hpt. 49. § (3)-(6) bekezdései sorolják fel azokat az eseteket, amikor az üzleti titok kiadható, egyébként az üzleti titok is szigorúan bizalmasan kezelendő.

A banktitok és üzleti titok Hpt-ben található néhány közös szabályát azért érdemes szó szerint idézni, mert ezek már a felhőszolgáltatási szerződés tartalmára is kihatnak:
„55. § (1) Aki üzleti vagy banktitok birtokába jut, köteles azt időbeli korlátozás nélkül megtartani.
(2) A titoktartási kötelezettség alapján az üzleti, illetőleg a banktitok körébe tartozó tény, információ, megoldás vagy adat, az e törvényben meghatározott körön kívül a pénzügyi intézmény, illetve az ügyfél felhatalmazása nélkül nem adható ki harmadik személynek, és feladatkörön kívül nem használható fel.
(3) Aki üzleti titok vagy banktitok birtokába jut, nem használhatja fel arra, hogy annak révén saját maga vagy más személy részére közvetlen vagy közvetett módon előnyt szerezzen, továbbá, hogy a pénzügyi intézménynek vagy az intézmény ügyfeleinek hátrányt okozzon."
Az (1) bekezdésből az következik, hogy a felhőszolgáltatási szerződésnek a titoktartásra vonatkozó rendelkezései – legalábbis az üzleti- és banktitkok vonatkozásában – a szerződés megszűnését követően is korlátlan ideig kötik a feleket: a szerződésben erre mindenképpen ajánlott kifejezetten utalni. Épp ez teszi többek között lényeges kérdéssé, hogy az adatbiztonság, így pl. az adatok helyreállíthatatlan törlése miként biztosítható a szerződés megszűnésekor, ahogyan erről korábban már esett szó.
A (3) bekezdés azért is érdemel figyelmet, mert világossá teszi, hogy ha a felhőszolgáltató jogsértő adatkezelése (adatfeldolgozása) nem ütközne a már tárgyalt (a Tőkepiaci tv-ben szabályozott) bennfentes kereskedelem tilalmába, akkor is létezik egy hasonló logika mentén kidolgozott, de sokkal általánosabb (ugyanakkor az Info tv. adatvédelmi szabályaihoz képest specializált) előírás, amely a nyereségszerzési (hátrány okozási) célzattal történő titoksértést tiltja.

Végül annak érdekében, hogy a kép teljes legyen, illetve, hogy a titoksértés kizárásának súlyát a felek érzékeljék, röviden meg kell említsük, hogy a banktitok megsértése akár büntetőjogilag is szankcionált cselekmény lehet. Ma már a Büntető Törvénykönyv a különböző titokfajták megsértését egy tényállásban tartalmazza, *„gazdasági titok megsértése"* címen, az alábbiak szerint:
„300. § (1) Az a bank-, értékpapír-, pénztár-, biztosítási vagy foglalkoztatói nyugdíjtitok megtartására köteles személy, aki bank-, értékpapír-, pénztár-, biztosítási vagy foglalkoztatói nyugdíjtitoknak minősülő adatot jogtalan előnyszerzés végett, vagy másnak vagyoni hátrányt okozva illetéktelen személy részére hozzáférhetővé tesz, úgyszintén aki jogtalan előnyszerzés végett, vagy másnak vagyoni hátrányt okozva üzleti titkot jogosulatlanul megszerez, felhasznál, mással közöl vagy nyilvánosságra hoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő."

6.6. A Hpt-ben előírt informatikai védelem

Pénzügyi intézménnyel tervezett szerződéskötés esetén nagyon lényeges annak tudatában előkészíteni a megállapodást és vállalni az abból eredő kötelezettségeket, hogy maga a Hpt. – függetlenül attól, hogy történik-e bármiféle kiszervezés – nagyon komoly informatikai védelemre vonatkozó szabályokat tartalmaz, amelyek a felhőszolgáltató szakmai tevékenységét is befolyásolják.
A Hpt. 13/C. § (1) bekezdése szerint: *„A pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer*

biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén."

Ez az előírás azért kap jelentőséget a felhőszolgáltatások terén, mert a szolgáltató tudomásul kell vegye, hogy a felhasználónál hatályban van egy informatikai biztonsági szabályzat (amelyen – az alábbiakban idézett 13/C. § (5) és (6) bekezdéseiből következően – többféle informatikai biztonsági célú dokumentumot értünk), amelynek érvényesüléséről a pénzügyi intézmény a kiszervezett tevékenységek kapcsán is köteles gondoskodni. Praktikusan e szabályzat (illetve ennek egyes részdokumentumai) a szerződés mellékletét kell képezze.

További Hpt. által támasztott követelmény, hogy a pénzügyi intézmény legalább két évenként felülvizsgálja és aktualizálja az informatikai rendszer biztonsági kockázatelemzését. Ez az elemzés a felhőszolgáltatási szerződés hatályba lépésétől kezdődően értelemszerűen kiterjed majd a felhőszolgáltató tevékenységére is, amely a felek között nemcsak általános értelemben vett, hanem igen mély szakmai együttműködést feltételez. Ez a kockázatelemzés felfogható a szolgáltatás minőségének folyamatos kontrolljaként is, így a felhasználói oldal elemi érdeke, hogy erre a szerződés rendelkezést tartalmazzon s ez a gyakorlatban is megtörténjen.

A pénzügyi intézmény oldalán továbbá felmerülhet annak szükségessége, hogy addig alkalmazott szabályozási rendszerét is felülvizsgálja és arra tekintettel aktualizálja, módosítsa, hogy a felhőszolgáltatással egy újszerű (tehát egyes vonatkozásokban még nem szabályozott), fokozott kockázatokat rejtő informatikai biztonsági probléma jelenik meg a rendszerben.

Nem is annyira jogi, mint inkább informatikai-szakmai szempontból bírnak jelentőséggel a Hpt. 13/C. § (5) - (9) bekezdései[19], amelyek egyfajta minimumelvárásokat rögzítenek,

[19] (5) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:
a) a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról,
b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról,
c) a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események),
d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére,
e) a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről,
f) az adathordozók szabályozott és biztonságos kezeléséről,
g) a rendszer biztonsági kockázattal arányos vírusvédelméről.
(6) A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:
a) informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel,
b) minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működését - még a szállító, illetőleg a rendszerfejlesztő tevékenységének megszűnése után is - biztosítja,
c) a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb - a tevékenységek, illetve szolgáltatások folytonosságát biztosító - megoldásokkal,
d) olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását,
e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről,
f) jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizzék,
g) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.
(7) A pénzügyi intézménynél mindenkor rendelkezésre kell állnia:
a) az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek,
b) az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének,

továbbá a felhőszolgáltatási szerződés kapcsán arra világítanak rá, hogy melyek azok az informatikai szakmai keretek (illetve az azokat tartalmazó szabályzatok), amelyekhez a felek feltétlenül kötelesek alkalmazkodni:

6.7. Kizárólagosság kikötése

A Hpt. általános bemutatása során már érintettük, hogy a felhőszolgáltatásra a „kiszervezés" Hpt. szerinti szabályai alkalmazandók. A kiszervezésnek pedig az a fajtája, amely „adatkezelés, adatfeldolgozás vagy adattárolás" megvalósítására is irányul, azaz, amelyhez a felhőszolgáltatás is sorolható, a Hpt. e rendelkezése szerint „kizárólagos" szerződés alapján folytatható. Ennek megfelelően a szerződésnek tartalmaznia kell, hogy a felhőszolgáltatóhoz kiszervezett tevékenységre az adott szolgáltató – nyilvánvalóan a szerződés hatálya alatt – kizárólagosan jogosult (negatívan megfogalmazva: a pénzügyi intézmény azonos tevékenységre egyidejűleg egy felhőszolgáltatóval szerződhet, szemben a felhőszolgáltatóval, amely akár több pénzügyi intézmény számára is nyújthatja egyidejűleg szolgáltatásait).

6.8. Alkalmazandó jog, kikötött bíróság

Az alkalmazandó jog és eljáró bíróság kikötésének természetesen akkor van létjogosultsága, ha a szerződés olyan nemzetközi elemet tartalmaz, amely kérdésessé teszi az irányadó jogot. Kiindulási pontunk az volt, hogy a 6. fejezetben írtakat magyar illetőségű szerződő felek Magyarországon végzett szolgáltatások tárgyában kötött szerződéseire lehet alkalmazni. Ha ezek valamelyike nem teljesülne, kérdésessé (vagy kizárttá) válna, hogy a Hpt. alkalmazható legyen a jogviszonyra, márpedig a jogalkotó szándéka kétségtelenül az volt, hogy a Hpt. kógens rendelkezései (amelyektől a felek megállapodása nem térhet el) érvényesüljenek kiszervezett tevékenység esetén is. Megítélésünk szerint ezért a szerződésnek – ha a magyar joghatóság és jogrend alá tartozása nem magától értetődő – nem mellőzhető eleme a magyar jog, mint irányadó jog és valamely magyar bíróság illetékességének kikötése (arra figyelemmel azonban, hogy a Polgári Perrendtartás alapján nem köthető ki a helyi bíróságok közül a Pesti Központi Kerületi Bíróság és a megyei bíróságok közül a Fővárosi Törvényszék, valamint a Budapest Környéki Törvényszék).

---

c) az informatikai rendszer elemeinek a pénzügyi intézmény által meghatározott biztonsági osztályokba sorolási rendszerének,
d) az adatokhoz történő hozzáférési rend meghatározásának,
e) az adatgazda és a rendszergazda kijelölését tartalmazó okiratnak,
f) az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek,
g) az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.
(8) A szoftvereknek együttesen alkalmasnak kell lenni legalább:
a) a működéshez szükséges és jogszabályban előírt adatok nyilvántartására,
b) a pénz és az értékpapírok biztonságos nyilvántartására,
c)129 a pénzügyi intézmény tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra, ideértve a pénzforgalmi számlák cégbíróság felé történő bejelentését is,
d) a tárolt adatok ellenőrzéséhez való felhasználására,
e) a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.
(9) A pénzügyi intézménynek belső szabályzatában meg kell határoznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.