Szemelvények a katonai műszaki tudományok eredményeiből III.

Szerkesztette
Földi László

LUDOVIKA
EGYETEMI KIADÓ

Szemelvények a katonai műszaki tudományok eredményeiből III.

Szemelvények a katonai műszaki tudományok eredményeiből III.

Hallgatói kötet

Szerkesztette

Földi László

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2022

Szerzők

Albert Gábor
Bakos Tamás
Bencsik Gábor
Berta Katalin
Deli Gábor
Domán László
Gajdács László
Győző-Molnár Árpád
Horváth Attila
Horváth Ákos
Igaz-Danszky Tamás
Jagodics Ibolya
Kersák József Zsolt
Kiss Ádám István
Kovács Gergely
Kovács-Horváth Adrienn
Kutassy Emese
Lakatos Bence R.
Leskó György
Lévai Zsolt
Major Gábor
Marlok Tamás
Matusz Márk Péter
Szabadföldi István
Szajkó Gyula
Szilágyi Tibor
Tamás Enikő Anna
Teknős László
Terék Tamás
Tímár Attila
Tóth Bence
Vass Gyula

Lektorok

Berek Tamás
Bíró Tibor
Haig Zsolt
Horváth Attila
Kátai-Urbán Lajos
Németh András
Padányi József

Ludovika Egyetemi Kiadó
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Deli Gergely rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: György László
Korrektor: Bíró Csilla, Pokorádi Zsófia
Tördelőszerkesztő: Stubnya Tibor

ISBN 978-963-531-703-5 (elektronikus PDF) | ISBN 978-963-531-704-2 (ePub)

Tartalom

Jagodics Ibolya

A felhőtechnológia adatvédelmi megfelelősége a GDPR fényében

Absztrakt

Az információs társadalom igényeit kiszolgáló technológia trendjei az Ipar 4.0 dinamikus világában több olyan újdonságot és kihívást teremtenek, amelyek között az információ mennyisége és kezelése, tárolása egyaránt sarkalatos pontok. Az információ értéke, így biztonsága és elérhetősége kiugróan fontossá vált. Napjainkra már megoldást jelent a hatalmas adatok kezelésére és tárolására a felhőalapú technológia. Azonban felmerül a kérdés, hogy ez mit is rejt önmagában, hol található, és valóban biztonságos-e ebben kezelni, tárolni az adatokat. Szintén kérdéses, hogy a General Data Protection Regulation, amely 2016 óta a szolgáltatókat szabályozza az adatok kezelésének terén, vajon megfelelő hátteret nyújt-e a felhőtechnológia alkalmazásához, illetve a szolgáltatók GDPR-megfelelése megteremti-e a felhasználók személyes adatainak védelméhez szükséges biztonságot. Jelen munkámban ezekre a kérdésekre keresem a választ.
Kulcsszavak: *felhőalapú technológia, GDPR, információ, megfelelőség, szabályozás*

GDPR Related Privacy Compliance of Cloud Technology

The technology trends that serve the needs of the information society in the dynamic world of Industry 4.0 generate several innovations and challenges, where the amount of information and its management and storage are crucial points. The value of information, thus its security and availability have become highly important by now. Cloud technology serves as a solution for the data management and storage. Nevertheless, the question arises: what is this cloud technology at all, and whether it is safe enough to manage and store data within it? A further question is if the GDPR, which has been regulating the service providers in terms of personal data management since 2016, provides an appropriate background for the application of cloud technology. Does the service providers' GDPR conformity establish enough security for the end-users' personal data? I seek answers for these questions in my present work.
Keywords: *cloud technology, GDPR, information, conformity, regulation*

Bevezetés és kutatási részletek

Az elmúlt évek tapasztalati szerint az állandóságot keressük, viszont az állandóság a folyamatos változásokban mutatkozik meg. A versenyképesség előfeltétele a rugalmasság, az alkalmazkodás, továbbá a változásokból eredő nehézségekkel szemben az új lehetőségek felismerése, kiaknázása.

Magyarországon – témám szempontjából – az egyik lényeges változás volt a személyes adatok védelmének érdekében 2016-ban megjelent, majd 2018-ban hatályba lépett Általános Adatvédelmi Rendelet. Ez a szolgáltatókat szorítja szigorú szabályok közé a felhasználók adatainak védelme érdekében, és körültekintésre készteti a magánszemélyeket.

Más releváns változás a felhőalapú technológia megjelenése. A felhő maga az az új tárhely, adatkezelési megoldás, amely fizikailag nem megfoghatóan az elektromágneses spektrumot is felhasználó kibertérben található.

Napjainkban az információ és az idő az információs társadalom legértékesebb eleme. A szolgáltatók adatvédelmi megfelelése és szabálykövetési magatartásuk kritikus pontja a kibertér feltételezhető sérülékenységének.

Vizsgálatomban empirikus elemzés segítségével a General Data Protection Regulation – GDPR vagy Általános Adatvédelmi Rendelet – által dedikált alapelvek és jogok[1] fellelhetőségét vetem össze három választott multinacionális vállalat felhőalapú tárhelyszolgáltatásra hivatkozott publikus szabályzataival. Azért, hogy a szolgáltatók tájékoztatói alapján minősíteni tudjam a felhasználók adatainak védelmét a rendelet értelmében.

Felhasznált irodalomként magyar szakirodalomra támaszkodom a GDPR-rendelet és a felhőalapú szolgáltatások bemutatására, az elemzéshez pedig a vállalatok által nyilvánosságra hozott – angol nyelvű – elektronikus dokumentációt használom. A munka a Magyarországon működő és hazai felhasználók szempontjából lényeges elemekre terjed ki. A téma jogi vetületei nem képezik jelen munka témáját.

A GDPR

Az Általános Adatvédelmi Rendelet[2] története az 1949. évi XX. törvénnyel[3] kezdődött. Ebben írták le, hogy mindenkit megillet a személyes adatok védelméhez fűződő jog. Az információ szerepének felértékelődése miatt az országgyűlés 1992. november 17. napján közzétette az adatvédelmi törvényt (1992. évi LXIII. törvény[4]), útmutatásként a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. Ennek módosítása tartalmazta a 95/46/EK irányelvet,[5] amely a 2011. évi CXII. információs törvény[6] megfelelője az információs önrendelkezési jogról és az információszabadságról hazánkban. Majd az Európai Parlament és a Tanács (EU) 2016/679 rendelete 2016. április 27. napján hatályon kívül helyezte a 95/46/EK irányelvet, és kiterjesztette a természetes személyek adatkezelésének, illetve az adatok szabad áramlásának szabályozását. A rendelet kétéves

[1] Az alapelveket és jogokat a II. fejezetben kifejtik, ezek megjelenését a szolgáltatók szabályzataiban a III. fejezet tartalmazza.

[2] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete. 2016. április 27.

[3] 1949. évi XX. törvény. A Magyar Népköztársaság Alkotmánya.

[4] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

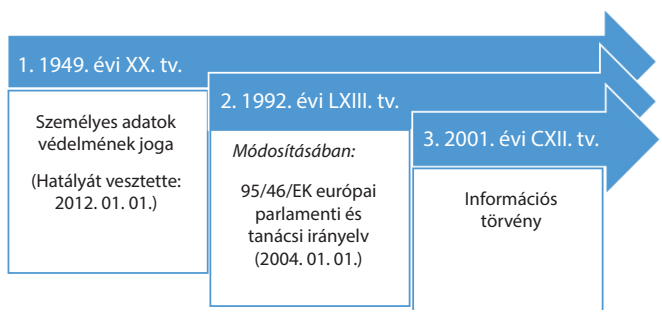
[5] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. 1995.

[6] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

türelmi időszak után 2018. május 25. napjától lépett életbe Magyarországon. A GDPR az Európai Unió által egységesített és az egyének adatvédelmét keretbe foglaló szabályozás, az EU területén működő gazdasági szereplőket szabályozza a személyes adatok kezelése, tárolása, továbbítása terén.

Kiemelve a 2016/679 rendelet 5. cikkét, a továbbiakban felsorolom a személyes adatok kezelésére vonatkozó *alapelveket:*

- jogszerűség;[7]
- tisztességes eljárás és átláthatóság;
- célhoz kötöttség;
- adattakarékosság;
- pontosság;
- korlátozott tárolhatóság;
- integritás és bizalmas jelleg;
- elszámoltathatóság;
- bizalom.



1. ábra: A GDPR kialakulása
Forrás: a szerző szerkesztése

A felsoroltak mutatják, hogy a meghatározott célú, kizárólag és minimálisan szükséges, továbbá bizonyos ideig tárolható adatok szabályozását merev keretek közé szorítja a rendelkező. A fenti elveket a szolgáltatók által rendelkezésre bocsátott információk alapján minősítem. A jogszerűség alapelvére külön nem nyújt kitekintést a munka, azt elfogadottnak tekintem a szolgáltatás biztosításának feltételei miatt.

Ezen túl fontos kitérni a 2016/679 rendelet 12–22. cikkeinek tartalmára. Ezek az érintettek jogait szabályozzák, amelyek a következők:

- tájékoztatáshoz való jog;
- hozzáféréshez való jog;
- helyesbítéshez való jog;
- törléshez és elfeledtetéshez való jog;

[7] A további elemzés nem ismétli az alapelvek és jogok felsorolását.

– korlátozáshoz való jog;
– adathordozhatósághoz való jog;
– tiltakozáshoz való jog;
– automatikus döntéshozatal elutasításához való jog.

A felhőalapú technológia

A felhő általános bemutatása

Napjainkban az információs társadalom és technológia kölcsönös függőséget valósít meg. Ezen technológiai fejlődés hozadéka maga a felhőalapú tárolás létrejötte. Folyamatosan és exponenciálisan növekszik a kezelt adatok mennyisége, bonyolultabb a továbbítás útja, ami a hálózatok közötti kapcsolatok és új tárolási megoldások felé mutatott mindaddig, ameddig megjelent a felhőalapú adattárolás. A felhőalapú számítástechnika a felhasználói igények kielégítését eddigi ismereteink szerint biztosítja, ugyanakkor nem vagyunk teljes mértékben tisztában működtetésének biztonsági feltételeivel, paramétereivel. A szolgáltatás igénybevételével rábízzuk magunkat a szolgáltatóra, hisz fentebb rávilágítottam arra, hogy a GDPR a szolgáltatókat szabályozza, akik üzemeltetik a felhőalapú szolgáltatást biztosító alkalmazásokat. Ugyanakkor a felhőnek az információbiztonság hármas elvén – vagyis a bizalmasságon, a sértetlenségen és a rendelkezésre álláson – túlmenően, az adatvédelmi szempontok szerint a természetes személyek jogait is biztosítania kell. Ezen megfelelések a felhőtechnológia kiépítése és működése során elsősorban a szervereket és adattárolókat, illetve az adatközpontokat érintik, tekintettel arra, hogy a szabályozás legfőképpen az ezekben tárolt, kezelt, használt adatokat védi.

A felhőalapú szolgáltatások *előnyei*[8] között egyértelműen a fejlődésnek köszönhető rugalmas méretezhetőség az elsődleges szempont, hisz a kibertér folyamatosan bővül, ezzel együtt a felhőben tárolt adatokhoz is gyakorlatilag a szükségleteknek megfelelő *méretet* biztosítanak. A tárhely elérhetőségi helyének köszönhetően korunk releváns elvárásait – mint az idő és gyorsaság – szintén garantálja. A magánszemélyek és vállalatok, kormányzati szervek adatállománya drasztikusan megnőtt, ennek kezelése jelentős költségtöbbletet generál, ami nem kedvez a gazdasági teljesítmény javításának. Így a felhőalapú tárhely alkalmazása a gazdaság szereplői számára a *költségek csökkentését* is elősegíti. A *valós idejű kommunikáció* megszünteti a mindannyiunk által ismert technikai vagy emberi hibák által okozott nehézségeket. Az adatok változtatásait azonnal menti a rendszer, így a kapcsolat megszakadása esetén nem tapasztalunk adatvesztést.

A felhőnek – mint minden másnak is – természetesen vannak *hátrányai,* amelyek a technológiai vívmányoknak köszönhetően minimálisak.

– Az elsődleges biztonsági kockázatot az emberi faktor adhatja, feltételezve a szolgáltató megfelelését, hiszen a szabályok betartása a felhasználó felelőssége.

[8] Miért menő a felhő és milyen előnyei vannak? *Business & Café,* 2016. április 24.

Amennyiben a szolgáltató a rá vonatkozó rendeleteknek és ellenőrzéseknek megfelel, ő felelősségre aligha vonható egy felhasználó általi hiba okozta hátrányos helyzetben, itt értve a rendelet által biztosított jogok védelmének elmaradását.

– További kockázatként értékelendő a rendelkezésre állás kimaradása, amely leginkább a kisebb, esetleg ismeretlen szolgálatóknál feltételezhető, illetve azon esetben, ha a tárhely szolgáltatója nem saját kapacitását bocsátja rendelkezésre, hanem úgynevezett harmadik fél bevonásával biztosít szolgáltatást.
– Utóbbi bizonytalansági tényező egyben következtetni enged a felhő elérhetőségének és sávszélesség-használati (technikai) nehézségeire is. A felhő eléréséhez[9] energiaforrást kell biztosítani, hogy az emberek és eszközök közötti kapcsolat létrejöjjön. Ezen túl a megfelelő sávszélesség biztosítása a kommunikáció sebességét befolyásolja. Nyilvánvalóan jelenleg is vannak olyan helyek a világon, gondoljunk például a hegyes területekre, ahol a legmodernebb technikai háttér sem biztos, hogy folyamatos kapcsolatot képes létesíteni a felhasználó és az információs technológia számára.

A DESI[10] 2018-as országjelentése alapján Magyarország Európában a 4G mobil kommunikációs technológia lefedettségében 91%-kal a 18. helyen szerepelt.[11] Ez 1 Gb/s adatátviteli sebességen működik, amivel magas szintű mobilitást, tíz néhányszor 100 Mbit/s adatsebességet és 10–25 km hatótávot biztosít mindössze 1 W teljesítménnyel.[12] Ugyan a felhő eléréséhez vezetékes kapcsolaton keresztül is csatlakoznak a felhasználók, az erősebb és gyorsabb kommunikációt a 4G is biztosítja, ezt tovább javítja az 5G megjelenése is. Az 5G kiépítése és lefedettsége még az előnyeinek ellenére sem teljes, azonban idővel várhatóan átveszi a 4G helyét, és elsődlegesen áll a felhasználók rendelkezésére.

A felhő típusai (a használat feltételei)

A felhőszolgáltatásokhoz való hozzáférés alapján három típust különböztetünk meg; a publikus, privát és hibrid felhőt.[13] A vállalatok felsorolnak egy negyedik típust is, a közösségi felhőt,[14] amely a publikus felhőhöz hasonlatos, közösségi igényeket elégít ki. Adatvédelmi szempontból fontos, hogy a szolgáltatók milyen adatokat használnak ezekben, miként garantálják az adatok védelmét a különböző felhőtípusokban. Ugyan a felhasználók bizonyos esetekben díjat fizetnek a használatért cserébe, az üzemeltetésből

[9] *Felhő alapú szolgáltatás. A felhő alapú szolgáltatás hátrányai.* (É. n.)

[10] *A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI), Magyarországról szóló országjelentés.* 2018.

[11] *A digitális gazdaság és társadalom…* (2018): i. m. 3.

[12] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. 106.

[13] Haig (2018): i. m. 91.

[14] Siim Alatalu: NATO's New Cyber Domain Challenge. In *2016 IEEE International Conference on Cyber Conflict.* (CyCon U.S.) 2016.

eredő kockázatok felelőssége továbbra is a szolgáltatóé. A felhasználó áthelyezi a felelősséget a fizetett díjért cserébe. Ezzel, ha az adatok jogosulatlan felhasználás, módosítás, törlés, visszaélés áldozatává válnak, a GDPR értelmében a sértett felhasználó panaszát, kárát érvényesítheti a szolgáltató felé. Fontos, hogy a jelenlegi piaci környezetben különböző jogi entitások eltérő megállapodások alapján osztozhatnak a szolgáltatás biztosításának menedzselésében. Az említett felelősség azon szolgáltatókat érintheti hátrányosan, amelyek az adatok menedzselését, továbbítását, feldolgozását végzik. A visszaélés lehetősége témám esetében az adatok továbbértékesítésére, üzleti titkok, érzékeny adatok feltárására irányul. Adatvédelmi szempontból a legbiztosabbnak tekinthető a privát felhő, amely egy konkrét szervezetet szolgál, így ebben az adatok kezelése és felhasználása egy kézben összpontosul. Így az adatkezelés felelősségi köre egyértelműen azonosítható. Ugyanebből a szempontból leginkább aggasztó a publikus felhő lehet a személyes adatok tekintetében, hisz ebben az adatok bárki számára elérhetők, azok a felhőt szolgáltatók kontrollja alatt állnak és tulajdonukat képezik. A közösségi felhő több szervezet használatában áll, a GDPR erre jól alkalmazható feltételeket szab meg. Az adatvédelmi kontroll állhat a szervezetek vagy akár a szolgáltató hatáskörében is. A hibrid felhő a publikus és privát felhő keveréke, amelyben a felhők jellegzetességei megmaradnak. Hibrid felhő esetében az adatok hordozhatósága kiemelkedően érvényesül, ám nehézséget okozhat az adatvédelem szempontjából e típus szövevényes felépítése.[15]

Említést tettem arról a 11.1. alfejezetben, hogy az információ értéke, az idő és gyorsaság már-már felbecsülhetetlen. A gazdaság szereplői igyekeznek minél egyszerűbb, gyorsabb, automatikusabb és olcsóbb megoldásokkal élni. Az adatkezelés olcsóbb formáját kínálja a felhőalapú technológia. Ügyféloldalon nem kell stábot fenntartani, a biztonsági szempontok és szabályok szerinti működés biztosítása és ellenőrzése a szolgáltatóhoz kerül. Ezen túl igényekre szabott a rendelkezésre állás, a tárhely méretei, ami a terjedő otthoni munkavégzés *(home office)* közegében egyre fontosabb. A modern megoldások, a gyors hozzáférés segíti az alkalmazottak időhatékony munkavégzését is. Hátrány azonban az ügyfél részéről biztosítandó technikai háttér feltétele.

A felhőszolgáltatás szintjei egymásra épülnek, alapvetően három típust ismerünk,[16] azonban a Microsoft egy kisegítő negyedik típust is piacra dobott, amelyekből a vevő választhat. Ezek a következők:

– Szoftverszolgáltatás (SaaS),[17] amelyben magát a szoftvert adja a szolgáltató, ilyen például a Google Docs, Drive.
– Platformszolgáltatás (PaaS),[18] amely az üzemeltetéshez szükséges környezetet szolgáltatja, ilyen a felület, a frissítések, például a Google App Engine.

[15] Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. *Hadmérnök,* 6. (2011), 4. 188.
[16] Haig (2018): i. m. 93.
[17] Software as a Service – SaaS.
[18] Platform as a Service – PaaS.

– Infrastruktúraszolgáltatás (IaaS),[19] amely maga a tárhely, a hálózati kapcsolat biztosítása, ilyen a Google Compute Engine.
– Kiszolgáló nélküli számítástechnika, amely az alkalmazások funkcióit építi ki, ezzel átvállalja a platformszolgáltatások manuálisan szükséges fenntartó tevékenységeit a felhasználótól.

GDPR a kibertérben

Az ember mesterségesen létrehozta a kiberteret, amely azon túl, hogy mesterséges és dinamikusan változó tartomány,[20] egyben hadszíntér is: a 2016-os varsói NATO-csúcstalálkozón ötödik hadszíntérként ismerték el. Az elektromágneses spektrumot és vezetékes kapcsolatokat is használja, ezekben kapcsolja hálózatba az eszközöket, teremt globális kapcsolatot és biztosítja az információ beszerzését, feldolgozását, felhasználását és továbbítását. A kibertér struktúrája az információs környezet három dimenziójával párhuzamba állítható, a fizikai, információs és kognitív dimenzióban. A fizikai dimenzió a kibertér fizikai rétegével feleltethető meg, amelyet földrajzi és hálózati komponensek alkotnak. Az információs dimenzió a kibertér logikai rétegét fedi le, amelyben logikai komponenst találunk. A kognitív dimenzió a kibertér kiberszemélyiség-rétegéhez hasonlítható, amelyben az interfész, a felhasználói és közösségi komponensek érvényesülnek.[21]

A felhőalapú technológia alkalmazása során a kibertér rétegeiben megjelennek az adatok, amelyek védelmére törekszik a GDPR. A kiberszemélyiség rétegében a felhasználói és interfészkomponensben kezelt, tárolt azonosítók, például az IP-cím (felhasználói komponens), a felhasználók saját hardver- és szoftvereszközei, mint például a laptop (interfészkomponens) vannak. A kiberszemélyiség közösségi komponensében rögzülnek a felhasználók hálózati interakciói, kapcsolati adatai. A logikai rétegben jelennek meg a felhasználók, szolgáltatók adatai, azonosítói, azon szabályok, protokollok, amelyekkel megfelelően működhet az információ kezelése, illetve az egyes szoftveres alkalmazások. A földrajzi elhelyezkedés (földrajzi komponens – fizikai réteg), az optikai/akusztikus/biológiai szenzorok által rögzített információ, mint a magánszemélyről rögzített kép, hangulati adat (hálózati komponens – fizikai réteg).[22] Ezekből látható, hogy a GDPR hatálya alá tartozó személyes adatok mindhárom rétegben fellelhetők. Nemcsak a személyt egyértelműen azonosító adatok, de azon adatok is védelem alá esnek, amelyekből a személyre következtetni lehet. Emiatt a szolgáltatóknak meg kell határozni, mely adatokat használják, hisz a szolgáltató működése során a különböző statisztikákhoz bizonyára rögzíti a felhasználó eszközazonosítóját, használati jellegzetességeit, aktivitását, hozzáfér a kamera vagy mikrofon által rögzített biometriai adatokhoz

[19] Infrastructure as a Service – IaaS.
[20] Haig (2018): i. m. 16.
[21] Haig (2018): i. m. 16.
[22] Haig (2018): i. m. 16.

is. Ugyanúgy, ahogy a helymeghatározáshoz a felhasználó földrajzi adatait, a közösségi oldalakon tanúsított aktivitását, kapcsolati hálóját is tárolja.

A GDPR adminisztratív módon ad a szolgáltatók számára keretet, amelyben az előbbiekben említett rétegekben megjelenő adatok használatát, tárolását, továbbítását megszabja. A szoftveres beállítások különböző biztonsági előírások, sztenderdek alapján automatikusan kiszűrik, megakadályozzák, megóvják a felhasználókat a támadások ellen.

A felhőszolgáltatás GDPR-szempontú elemzése

Ebben a fejezetben a Magyarországon egy potenciális felhasználó által választható legismertebb szolgáltatók közül a Google, a Microsoft és az IBM biztonsági protokolljait vizsgálom meg azért, hogy a következő pontban összevethessem megállapításaimat a GDPR elvárásaival.

A kiválasztott felhőszolgáltatók adatvédelemmel összefüggő szabályzatai

A Google LLC az amerikai tőzsdén jegyzett részvénytársaság, amelyet 1995-ben két PhD-hallgató álmodott meg mint *matematikai alapokon nyugvó keresőrendszert.* 1998-tól az információs technológiák iparágában működik. A Google számos tevékenysége és leányvállalata átszövi a világ kommunikációs és információs hálózatát. A Google vizsgált felhőalapú tárhelyszolgáltatása a Google Cloud.

Az International Business Machines Corporation (IBM) egy 1911-ben alapított, amerikai székhelyű multinacionális informatikai cég. Az információs technológiák iparágában a *hardveralapú kínálata* a legszélesebb. Az adatfeldolgozás automatizálását megcélozva 1886-ban feltalálták a lyukkártya-feldolgozó gépet, s ez inspirálta a vállalat létrehozásának gondolatát.[23] Az IBM által nyújtott felhőszolgáltatás neve az IBM Cloud.

A Microsoft Corporation az amerikai tőzsdén jegyzett *szoftvervállalat.* 1975-ben alapították Új-Mexikóban. Ismert termékei a Microsoft Windows, Microsoft Office és az Xbox-termékek.[24] A Microsoft Azure terméke nyújt felhőalapú szolgáltatást a felhasználók számára,[25] amelyet az alábbiakban összevetek az IBM és a Google Cloud hasonló szolgáltatásával.

A Google LLC tájékoztatója áttekinthető, részletes információs halmazt ad a kereső számára arról, hogy miként felel meg a GDPR szabályainak. A Google LLC Általános Felhasználási Feltételek – ÁFF[26] című dokumentumát vizsgálom. Ebben külön-külön fejezetekben szól a szabályokról mind az ügyfélre, mind a partnerre és a technikai cél-

[23] IBM: *History of Progress.* 2008.
[24] History.com Editors: This day in history – Microsoft founded. A&E Television Networks, 2015.
[25] Az Azure a Microsoft felhőalapú szolgáltatásának fantázianeve.
[26] *Google Cloud & the General Data Protection Regulation (GDPR).* (É. n.)

csoportra vonatkozóan. Az általános és felhőspecifikus felhasználási feltételek mellett a támogatási lehetőségekre, a szolgáltatási megállapodásra, az egyedi esetekre, az Európára vonatkozó szerződési záradékokra és a compliance tényezőkre is kitér.

Az IBM felhőszolgáltatásának GDPR-értelmezése (frissítése hatályos: 2020. 12. 15-től) azt mutatja, hogy a cég ügyfélközpontú, könnyedén áttekinthető iránymutatást alkotott. Feltűnő a dokumentum olvasása során, hogy hangsúlyt fektetett a kezelt adatok típusaira és azok szükségszerűségének magyarázatára, számos példával alátámasztva.

A Microsoft a Google LLC gyakorlatához hasonlóan alapvetően az információvédelmi rendelkezések között tünteti fel a GDPR-értelmezését. Az Általános Szerződési Feltételekben elérhető egyéb hivatkozások világítanak rá a GDPR-hoz köthető további részletes információkra. Emiatt struktúrájában szövevényesebb halmaz áll a felhasználó rendelkezésére az adatvédelem megértéséhez.[27]

Alapelvek és jogok megjelenése a vizsgált szabályzatokban

Az alábbi részek az első fejezetben felsorolt (a GDPR 5. cikke szerinti) adatkezelési alapelvek és az egyén (a GDPR 12–22. cikkei szerinti) jogainak összevetését tartalmazzák, a mintákkal.

Alapelvek

Tisztességes eljárás és átláthatóság

Mindhárom szolgáltató oly módon biztosítja a fenti elveket, hogy az adatvédelmi értelmezését, gyakorlatát publikusan rendelkezésre bocsátja. A dokumentumok bevezetésében együttesen tisztázzák az alkalmazandó fogalmakat. Globális szolgáltatók lévén kitérnek a *területi eltérésekre,* vagyis a GDPR *hatálya* alá tartozó országokra, illetve a Svájcra és az Egyesült Királyságra vonatkozó különböző törvényekre. A cégek mindegyike létrehozott *szakértői csoportot* a GDPR-ral kapcsolatos ügyféltámogatás céljából.

A Google LLC az ÁFF-dokumentumában[28] többször hivatkozik arra, hogy a központi adatkezelési rendszerben az ügyfelek hozzáférhetnek az adataikhoz, illetve módosíthatnak rajtuk és rendelkezhetnek azokról. A leírás 12. pontja szögezi le azt is, hogy a cég ellenőrző szerv kérésére a GDPR-ral összefüggésben lévő adatokat a rendelkezésére bocsátja. A szolgáltató továbbá említést tesz a hálózatok és az adattovábbítás kitételeire is. Az ügyfél biztonságérzetét erősítve és a fenti elvet szem előtt tartva – a részleteket mellőzve ugyan, de – említést tesz a külső támadások elleni védelmi intézkedéseiről, ezek megelőzésére alkalmazott metodikájáról. Szót ejt továbbá a titkosításról. Az ÁFF

[27] Microsoft Corporation: *Microsoft Online Services Privacy Supplement (DPA).* (É. n.)
[28] *Google Cloud & the General…* (é. n.): i. m.

8. pontjában tájékoztat arról, hogy biztonsági kontrollokat, dokumentumokat biztosít, és ezek ügyfél általi hozzáférhetőségét garantálja.

Az IBM világos direktívát[29] ad a tevékenysége során kezelt adatok feldolgozása, továbbítása és tárolása részleteiről. Szintén működtet központi adatkezelési rendszert, amelyen keresztül az ügyfelek hozzáférhetnek, módosíthatnak és rendelkezhetnek a GDPR hatályába tartozó adataik felett.

A Microsoft által kiadott DPA harmadik melléklete további, GDPR-ral kapcsolatos szabályozási keretet határoz meg az *Európai Unió Általános Adatvédelmi Rendelet Kikötések* címmel.[30] Ebben – részletekbe nem menően – értesíti a felhasználót arról, hogy az adatokat kizárólag a meghatározott írásbeli jóváhagyást követően szerzett jogosultságokkal rendelkezők kezelik a vállalat részéről.

Elszámoltathatóság és bizalom

A cégek a különböző *ellenőrzéseknek* szükség szerint eleget tesznek az adatvédelem érdekében, erre a megszokott módon lehetőséget kínálnak, attól nem zárkóznak el. Az IBM naplót vezet a kezelt adatokról, az azokkal kapcsolatban felmerült problémákról és ezek kezelésének kritikus pontjairól. A naplót elérhetővé teszi, és biztosítja a megfelelő szervek és az ügyfél számára az ellenőrzési tevékenység elvégzését mind külső-, mind belsőtárhely-szolgáltatása esetén.

Mindegyik felhőszolgáltató felsorolja, illetve megjelöli, mely jogosítványok birtokában biztosít szolgáltatást az adatvédelem szabályait követve.

A Google szabályzata[31] 2. számú mellékletének 2. pontja részletezi a hozzáférési és helyszíni kontrollokat. Ebben az ügyfél tájékoztatást kap arról, hogy a vállalat minden fizikai adatközpont biztonságát 24 órás védelemmel, automatikus jelzőrendszerekkel, illetve CCTV zárt hálózatban működő, dedikáltan biztonsági szakemberek felügyeletével látja el. Ezen szakemberek folyamatos belső és külső tesztek alá vetik a rendszert, hogy megbizonyosodjanak annak sérülékenységéről, működőképességéről.

Adattakarékosság, célhoz kötöttség, korlátozott tárolhatóság és pontosság

Az előbbiekben említett hozzáférési és helyszíni kontrollok esetében a Google meghatározza az optikai felvételek tárolási idejét is, amelyet 30 napban definiál. A személyes, illetve kezelt adatok tárolhatóságát is megjelöli, ebben a tárolhatóság az ügyfél általi törlés idejéig terjed. Az adatok törlésére többlépcsős jóváhagyási megoldást tesz lehetővé, amelyben a törlésre vonatkozó információkat tárolja, ennek visszakövethetőségére

[29] IBM: *General Data Protection Regulation (GDPR).* 2022.
[30] Microsoft Corporation (é. n.): i. m.
[31] *Google Cloud & the General…* (é. n.): i. m.

riportokat archivál a törlést követően is. A Microsoft a törlés idejét a szolgáltatás megszűnését követő 90 napban,[32] az IBM pedig 2 napban határozza meg.[33]

Az ÁFF 2. számú mellékletének 3. pontja[34] az adatokról szól. Ebben kifejti az ügyfél által beállított adatok kezelésének szabályait – a Google ebben a mellékletben kifejezetten az ügyfél által megadott és kezelhetővé jelölt adatok kezelésére ad módot.

Az IBM adatvédelmi értelmezése definiálja a személyes adatok körét, ezek osztályozását.[35] A személyes adatok közé sorolja általában az identitásra és a családi állapotra, a magán- és szakmai életre vonatkozó adatokat, a helyadatokat, a csatlakozási adatokat és az eszköz adatait. Ezenkívül a személyes adatok típusait is kifejti, amelyek a következők:

- alapadatok (például a név, cím, telefonszám, e-mailcím);
- technikai adatok (például az IP-cím, az eszköz száma);
- foglalkoztatással kapcsolatos adatok (például a munkakör, munkahely, teljesítményértékelés);
- személyiséggel kapcsolatos adatok (például a hangulatelemzés);
- pénzügyi információk (például a hitelkártya, bankszámla, fizetési információk, szokások);
- egészségügyi adatok (fizikai és mentális egyaránt);
- tartózkodási hely információi;
- viselkedési biometriák a minták és nem az egyén azonosítására;
- kommunikációs adatok (például a képek rögzítése, audió- és/vagy videókonferencia-adatok, ebben hívásnaplók [az egyén hívásadatai], hozzáférési kódok és egyéb kommunikációs metaadatok).

Az adatok csoportosításának megfelelően kiemeli az érzékeny személyes adatok[36] körét is, mint például az egészségügyi adatokat.[37] A személyes adatok különleges kategóriáját is bemutatja, ezek feltárják az egyénre vonatkozó alábbi információkat:

- faji, etnikai adatok;
- politikai vélemény, politikai hovatartozás;
- vallási, filozófiai meggyőződés;
- genetikai;
- biometrikus;
- egészségügyi;
- nem, szexuális irányultság, aktivitás.

[32] Microsoft Corporation (é. n.): i. m.
[33] IBM (2022): i. m.
[34] *Google Cloud & the General…* (é. n.): i. m.
[35] IBM (2022): i. m.
[36] Sensitive Personal Data – SPD.
[37] IBM (2022): i. m.

A felhőszolgáltató szerződött ügyfeleitől megkívánja, hogy érzékeny adatok használatának esetére előre értesítse a szolgáltatót, illetőleg kezdeményezze egy külön klaszterbe soroláshoz szükséges eljárását. Ezen klaszterek esetében az IBM tájékoztat arról,[38] hogy az adatellenőr nevét és e-mailes elérhetőségét tárolja rendszereiben.

A szolgáltató összefoglalja a feldolgozási tevékenység elemeit, amelyekhez szükséges adatokat használnia, például az ügyféltámogatást, a minőségjavítást segítő, illetve az adatok továbbításához szükséges információkat.

A Microsoft Azure szolgáltatásában kiemelten kezeli az adatok osztályozására, védelmére, láthatóságára, kontrolljára, integrációjára, rugalmas kezelésére, megosztására utaló központi elveket, néhány szóval magyarázva azok értelmét. Mindezek az információk segítik a felhasználót döntésében, a szolgáltató által nyújtott felhőalapú megoldások mellett.

A DPA[39] alapvető útmutató a folyamatokhoz, azonban második számú melléklete (ÁSZF feldolgozók számára) fejti ki bővebben, mely típusú adatok szükségesek a szolgáltatás biztosításához. Az adatok kategóriáit külön deklarálja, ezek lefedik az IBM kategóriáit, azoknál bővebb, megtaláljuk benne a használt és tárolt ügyféladatok példáit is. Ezek közül néhányat a teljesség igénye nélkül az alábbiakban felsorolok:

- hitelesítés adatai (jelszavak, felhasználónév, PIN-kódok, biztonsági kérdések);
- elérhetőségi adatok (például cím, telefonszám);
- egységes azonosítószámok és aláírások (például bankszámlaszám, biztosítási szám, útlevélszám és személyiigazolvány-szám, jogosítványszám);
- internetezési tevékenység.

Az adattípusok példáit az alábbi kategóriákba sorolta a Microsoft:

- ügyféladatok (az ügyfél által biztosított adat);
- diagnosztikai adatok (ügyfél által telepített szoftverből kigyűjtött adat);
- szolgáltatás által generált adatok;
- szakmai szolgáltatási adatok (ügyfél által megadott adat a szakmai szolgáltatással kapcsolatban);
- támogató adatok (technikai támogatással összefüggésben ügyféltől érkező adat).

Integritás és bizalmasság

Mindhárom vállalat biztosítja partnereit, ügyfeleit, üzlettársait arról, hogy – együttműködésben és összehangban az elvárt törvénykezéssel – garantálja a folyamatok ismeretét, az adatok továbbítását, bizalmas kezelését, különböző jogosultságokhoz kötötten azok elérhetőségét. Részletezi, mely országokban mely törvény rendelkezéseit tekinti magára kötelező érvényűnek, és ezt miként valósítja meg. Külön bekezdéseket szentel a harmadik felekkel való együttműködés kereteinek tisztázására, a jogok és kötelezettségek sarkalatos pontjainak dedikálására.

[38] IBM (2022): i. m.
[39] Microsoft Corporation (é. n.): i. m.

A szolgáltatók frissített GDPR-dokumentuma biztosítja ügyfeleit, illetve partnereit arról, hogy különböző hitelesítési módszerekkel garantálja a rendszerhez, adatokhoz való hozzáférés korlátozását, felügyeletét.

Jogok

A *tájékoztatáshoz való jogot* elfogadottnak tekinthetjük, hiszen a szolgáltatók oldalán elérhetők a felhőszolgáltatásra vonatkozó kitételek. A szolgáltatók nyilvánosan közzétett értelmezései, illetve az adatvédelmi csoportok létrehozása, rendelkezésre bocsátása garantálják a tájékoztatást.

A tájékoztatók között mind a három szolgáltató megadja a szükséges hivatkozásokat, illetőleg információkat, amelyek meggyőznek arról, hogy adataikhoz a *felhasználók hozzáférhetnek,* s azt miként tehetik meg. Erre külön adatközpontot, szakértői hátteret biztosítanak. A jogosultak meghatározott köre számára bizonyos feladatok ellátását és ezekhez szükséges hozzáféréseket szab ki (például ellenőrzési feladatok ellátása, hozzáférési jogosultság kezelése). Az ügyfelek és ellenőrző szervek számára az ellenőrzés lehetőségét és az ehhez szükséges információkat biztosítja. Az IBM az adatközpontok mögött álló országok, szervezetek listáját szintén elérhetővé teszi.

A *helyesbítéshez való jog* alapján a felhasználó saját döntési hatáskörében a megfelelő felületen frissítheti adatait. Ezen a felületen, amelyre csak a felhasználó jogosult belépni a meghatározott jogosultság alapján, szintén maga dönthet adatainak módosításáról és törléséről. A felhasználónak így lehetősége és jogosultsága van adatain módosítani.

Az *adathordozhatóság jogának* tekintetében mindhárom szolgáltató külön szakaszban tárgyalja szabályait. Kitűzött cél részükről a törvényeknek való megfelelés. Ebben szintén kikötik, hogy a saját üzleti és működési folyamataikhoz szükséges adatok hordozhatóságával élnek.

A felhőszolgáltatást igénybe vevők a *tiltakozás jogát* oly módon gyakorolhatják, hogy a cégek egy dedikált belső osztályt biztosítanak a kérdések, kétségek megválaszolására, amely a Google esetében 24 órában elérhető online szolgáltatás. Ezenkívül bemutatják a panaszkezelés intézményét is.

Felhőszolgáltatás és a GDPR-megfelelőség értékelése

Az első négy alfejezet betekintés nyújtott a felhőalapú technológia világába, a GDPR megfelelőségébe, felvázolta az abban megfogalmazott alapelveket és jogokat, továbbá a három kiválasztott szolgáltató nyilvánosan közzétett szabályai mentén megvizsgálta utóbbiakat. *A felhőszolgáltatás GDPR-szempontú elemzése* című fejezetben betekintést kaptunk a három kiválasztott szolgáltató által nyilvánosságra hozott információkról a tárhelyszolgáltatásukat illetően, amelyeket összevetettem a GDPR 5. és 12–22. cikkeiben felsorolt alapelvekkel és jogokkal.

Mindhárom szolgáltató friss információkkal látja el a felhőalapú szolgáltatásokat igénybe vevő vagy leendő felhasználókat. Ugyan jelen munka a dokumentumok létére, azok tartalmára szorítkozik, a vizsgált szolgáltatók számos releváns tudnivalót foglalnak ismertetőikbe. A három kiválasztott felhőszolgáltató mind a technológia iparágában jeleskedik termékeivel és szolgáltatásaival. A Microsoft tűnhet kivételnek, hiszen tájékoztatójában érezhetően sokkal inkább hagyatkozik a felelősségek definiálására, mintsem folyamatai részletezésére. A Google LLC szolgáltatására vonatkozó adatvédelmi folyamat leírása során hiányolható a tárolhatóság és törlés pontos idejének definiálása, a cég csupán a szolgáltatások igénybevételét veszi alapul e téren.

A Google tájékoztatójában[40] nem találtam részletes információt a kezelt adatok kategorizálására és ezek példáira. Ennek ellenére méltán feltételezhetem, hogy ezt valószínűleg belső folyamataiban – a másik két vállalathoz hasonlóan – részletezi. Ugyanakkor ennek hiányossága sértheti a GDPR 12–22. cikkeiben foglalt tájékoztatás jogát. Ez esetben hiányosságokat vélek felfedezni az adattakarékosság, a korlátozott tárolhatóság alapelveiben, továbbá a döntéshozatal elutasításához való jog tekintetében. Habár ellenőrzési ismeretek birtokában az ügyféladat általánosan elfogadott köre például az ügyfél neve, azonosító adatai (adószám, születési adatok), címek (lakhely, székhely, telephelyek), bankszámlaszámok, etnikai hovatartozás lehetnek. Ezt megerősíti az IBM és a Microsoft szabályzataiban alátámasztott osztályozás és példák sora.

Az ellenőrzési szempontok közül mérvadó, hogy a mindhárom vállalat által nyilvánosságra hozott dokumentumok, ellenőrzések eredményei, különböző jogosítványok kivétel nélkül frissek, nem több, mint néhány hónapja feltöltött dokumentumok. Ez mutatja, hogy a vállalatok együttesen szem előtt tartják a körültekintő magatartást és prudens működést ügyfeleiknek, illetve a törvényeknek való megfelelés érdekében.

Az IBM által alkalmazott adatvédelmi szabályok[41] áttekintése során felfigyeltem arra, hogy a Google[42] és a Microsoft[43] dokumentumaitól eltérő struktúrába, illetve megvilágításba helyezi a rendelkezést. Ezzel a struktúrával könnyebben követhető és átláthatóbb az irat tartalma.

Az elemzés tárgyává tett vállalatok a nemzetközi információ-, illetve informatikai biztonságot megkövetelő sztenderdeket igazolják, felsorolják és elérhetővé teszik.

A Google Cloud adatvédelmi megfelelőségének érdekében külön kitér az ÁFF 10. pontjában az adatok továbbításának módjára és lehetőségére (lásd 4. fejezet). Mindhárom globális szolgáltató az Európai Gazdasági Térség országaiban működők számára biztosít adatvédelmi jogokat, alapelveket, ezért az országok között átívelő kapcsolatok veszélyeztetettséget jelenthetnek. Ezen esetekben elvárható az adatkezelési megállapodások létrehozása. Azonban a felhasználók információbiztonsági tudatosságának fejletlenségéből és egyéb hibákból eredően ezek a megállapodások elmaradhatnak,

[40] *Google Cloud & the General…* (é. n.): i. m.
[41] IBM (2022): i. m.
[42] *Google Cloud & the General…* (é. n.): i. m.
[43] Microsoft Corporation (é. n.): i. m.

így megnő az incidensek, visszaélések és jogsértések valószínűségének esélye. A Google erre az eshetőségre külön záradékba való belépést vár ügyfeleitől. Amennyiben az adott ügyfél nem tesz eleget saját kötelezettségeinek, és nem él a záradékban foglalt szabályok elfogadásával, úgy a Google a felelősségét áthárítja ügyfelére az adatvédelmi kockázatok tekintetében.

Következtetés

Következtetésként elmondható, hogy a kiválasztott szolgáltatók a dokumentációs és folyamati elvárásokat teljesítik. Ugyanakkor a Google, amelyben kivételesen nagy tömegű információ kering nyilvánosan, magasabb kockázati szintet képvisel. A világhálón korábban megjelent adatok felülvizsgálata is teljes körben elvárt a GDPR-megfeleléshez, így ez komoly erőforrásbeli és folyamatszervezési kihívást jelent. Jelen elemzés erre nem terjedt ki, azonban érdemes lehet ennek további vizsgálata. Ebből eredően javasolt minden felhőszolgáltatónak teljeskörűen gondoskodni a korábbi adatokról, és az archiválásról is.

A felhőszolgáltatók leginkább saját eszközeikkel biztosítanak tárhelyet, hálózatot, kapacitást a felhasználói igények kielégítésének érdekében. Ettől függetlenül megtalálhatók külső vagy harmadik felek, amelyek a szolgáltatási tevékenységet támogatják.

A nagy szolgáltatók mellett kisebb cégek is igyekeznek részt szerezni az iparágban, és a lehetőségeikhez mérten kiépíteni és biztosítani felhőalapú szolgáltatást, ám ők méretükből eredően nehézségeket is okozhatnak a leendő felhasználók számára.

Jelentős veszély a személyes adatokkal való visszaélés, azonban ezekre, a vizsgált iratok alapján, felkészültek a cikkben szereplő szolgáltatók. Az *adatvédelem biztonsága* a GDPR által védett és biztosítandó jogok sértésének kockázatát hordozza. Ez a kockázat a GDPR-rendelkezés megsértése esetén kiszabható büntetési tételek révén pénzügyi kockázatot jelenthet a szolgáltatókra nézve; ebben hiányosságot nem észleltem.

Hiányosságként tekintek arra, hogy a szolgáltatók elérhető szabályzatai között ugyan megtaláljuk a működéshez szükséges nemzetközi sztenderdek hivatkozását és megszerzését, azonban ezen vizsgálatok jelentéseit, tartalmát nem teszik közzé a felhőszolgáltatók. Ezenkívül a Microsoft, a másik két vállalattól eltérően, nem hangsúlyozza külön adatvédelmi csoport elérhetőségét. Ezzel hátráltathatja a bizalmi alapelv elfogadtatását.

A vizsgálat alapján ajánlott az adatvédelmi szabályzatokban a pontos információk megjelölése is, mint például a törlésre, tárolásra vonatkozó napok száma. Ezenkívül minden tárhelyszolgáltatónak érdemes a kezelt adatok körét részletezni, azok használatát indokolni felhasználóik számára. Összességében a vizsgált szolgáltatók a rendelet által elvártaknak dokumentációs szempontból megfelelnek. Azonban fontos megjegyezni, hogy a dokumentáció a folyamatok létét, a megfelelésre való törekvést igazolja. Amennyiben a szabályzatok nincsenek megfelelően a szolgáltatásra szabva, vagy azokat nem frissítik folyamatosan, úgy a tájékoztatás sérülhet, és a szolgáltatás folytonosságát veszélyeztethetik. Ennek ellenére a folyamatok működésének hatékonyságát nem tudom megítélni, hisz ahhoz rá kellene látnunk a szolgáltatók belső működése során keletkező mintákra.

Felhasznált irodalom

1949. évi XX. törvény. A Magyar Népköztársaság Alkotmánya.

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI), Magyarországról szóló országjelentés. 2018. Online: https://ec.europa.eu/information_society/newsroom/image/document/2018-20/hu-desi_2018-country-profile-lang_4AA43283-EC48-996F-09918493E34A691F_52334.pdf

Alatalu, Siim: NATO's New Cyber Domain Challenge. In *2016 IEEE International Conference on Cyber Conflict.* (CyCon U.S.) 2016. Online: https://ieeexplore.ieee.org/document/7836609

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete. 2016. április 27. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679

Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. 1995. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A31995L0046

Felhő alapú szolgáltatás. A felhő alapú szolgáltatás hátrányai. (É. n.) Online: https://pccenter.hu/hu/felho-alapu-szolgaltatas

From the Garage to the Googleplex. (É. n.) Online: https://about.google/our-story/#:~:text=The%20Google%20story%20begins%20in,assigned%20to%20show%20him%20around.&text=In%20August%201998%2C%20Sun%20co,was%20officially%20born

Google Cloud & the General Data Protection Regulation (GDPR). (É. n.) Online: https://cloud.google.com/security/gdpr?fbclid=IwAR1ZQOpIax23XtNf91gkBkDd80TtR44eg3C-0VYmarUOXvOHX7y-B8qAel90

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

History.com Editors: *This day in history – Microsoft founded.* A&E Television Networks, 2015. Online: www.history.com/this-day-in-history/microsoft-founded (letöltés: 2022. 05. 12.)

IBM: *General Data Protection Regulation (GDPR).* 2022. Online: https://cloud.ibm.com/docs/Cloudant?topic=Cloudant-general-data-protection-regulation-gdpr-

IBM: *History of Progress.* 2008. Online: www.ibm.com/ibm/history/interactive/ibm_history.pdf www.history.com/this-day-in-history/microsoft-founded

Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. *Hadmérnök,* 6. (2011), 4. 176–188.

Microsoft Corporation: *Microsoft Online Services Privacy Supplement (DPA).* (É. n.) Online: https://azure.microsoft.com/en-us/services/information-protection/ MicrosoftOnlineServicesDPA(WW)(English)(Dec92020)

Miért menő a felhő és milyen előnyei vannak? *Business & Café,* 2016. április 24. Online: https://businessandcafe.blog.hu/2016/04/24/miert_meno_a_felho_es_milyen_elonyei_vannak

A Katonai Műszaki Doktori Iskolában folyó képzés és fokozatszerzés igen széles kutatási palettát jelent. A haditechnikai fejlesztések mellett – azokkal párhuzamosan – kiterjedt kutatások folynak a katasztrófavédelem és a vízügyi kérdések területén is. Úgy is mondhatjuk, hogy a doktori iskola három lábon áll.

Ez a sokszínűség nagy lehetőségeket rejt. Az eltérő tudományágakban kutató doktoranduszok közvetlenül látnak rá más tudományterületek módszereire, eszközeire, kutatási témáira, amelyekből új inspirációkat nyerhetnek. Általános jelenség ez a tudományos kutatásban, így ezeket a lehetőségeket mi sem hagyhatjuk ki.

A doktori iskolában folyó kutatásokkal szemben elvárás, hogy az új tudományos eredmények hasznot hozzanak. Ez a követelmény a doktori iskola mindhárom területére vonatkozik. Ez a kötet egyik eleme ennek a felelősségteljes munkának.