BUDAPESTI GAZDASÁGI EGYETEM

PÉNZÜGYI ÉS SZÁMVITELI KAR

SZAKDOLGOZAT

Gyephár Alexa
Nappali
Gazdaságinformatikus
Üzleti adatelemző informatikus

2021

BUDAPESTI GAZDASÁGI EGYETEM

PÉNZÜGYI ÉS SZÁMVITELI KAR

A GDPR hatása az Európai Unió tagállamaira, társult tagjaira és a velük kapcsolatban álló harmadik országokra

Belső konzulens: Dr. Honfi Vid Sebestyén

Külső konzulens: Kósa Zoltán

Gyephár Alexa
Nappali
Gazdaságinformatikus
Üzleti adatelemző

2021

NYILATKOZAT

Alulírott GYEPHÁR ALEXA ..... büntetőjogi felelősségem tudatában nyilatkozom, hogy a szakdolgozatomban foglalt tények és adatok a valóságnak megfelelnek, és az abban leírtak a saját, önálló munkám eredményei.

A szakdolgozatban felhasznált adatokat a szerzői jogvédelem figyelembevételével alkalmaztam.

Ezen szakdolgozat semmilyen része nem került felhasználásra korábban oktatási intézmény más képzésén diplomaszerzés során.

Tudomásul veszem, hogy a szakdolgozatomat az intézmény plágiumellenőrzésnek veti alá.

Budapest, 2021 év május hónap 12 nap

.....

hallgató aláírása

Tartalom

1. Bevezetés…….....5

2. A GDPR áttekintése……...7
   2.1. A GDPR gyökerei……...…7
   2.2. Mi a GDPR és melyek a fő céljai…….....12
   2.3. Hol tart ma a GDPR?.....23

3. A kiváltó okok……..……25
   3.1. Figyelmeztető jelek a világgazdaságban……...…26
   3.2. Személyes adat, mint árucikk……..….27

4. A megvalósítás…….29
   4.1. Felmérés és előkészítés…….29
   4.2. Ellenőrző szervek, szankciók……...31

5. Belül vagy kívül?.....33
   5.1. Az egyes tagállamok, társult tagok esete…….…….34
   5.2. EU szabály, de nem csak az EU számára…….……35
   5.3. Adattovábbítás harmadik országba……...38

6. A GDPR jövője……43

7. Összefoglalás……...48

8. Irodalomjegyzék……..50

1. BEVEZETÉS

George Orwell 1984 című regényének egyik szállóigéje, „Nagy testvér szemmel tart!”, talán aktuálisabb napjainkban, mint valaha. Azonban a könyvben szemléltetett disztópikus világkép a hétköznapi ember számára szerencsére még csak a jövőt lefestő rémkép lehet, de a modern idők szülöttei számára a folyamatos megfigyelés már nem újdonság és meglepetés. A technológia robbanásszerű fejlődése, az internet térhódítása, az okostelefonok nagy mértékű elterjedése mind ahhoz vezettek, hogy mindennapossá váljon a személyes adataink összegyűjtése, tárolása valamint viselkedésünk és szokásaink figyelése. Megtalálhatóak személyes adataink az állami intézmények, hatóságok és magánvállalatok nyilvántartásaiban is, amiket annak érdekében alkottak meg, hogy saját tevékenységüket segítség.

Naponta több százszor adjuk ki személyes adatainkat harmadik feleknek, úgy, hogy arról nem is tudunk. Az ilyen nyilvántartott személyes adatok mennyiségének hirtelen megnövekedésének következménye az is, hogy egyre több a személyes adatokkal való jogtalan visszaélés. Az ilyen jogsértő tevékenységek során sajnos, az adatok hatalmas mennyiségét figyelembe véve, rengeteg ember személyiségi joga sérül. Az utóbbi években egyre több ilyen botrányról hallhatunk, ahol emberek millióinak személyes adatait használták fel jogtalanul. Az egyik talán leghíresebb ilyen eset, a Cambridge Analytica botránya, amit a későbbiekben kicsit részletesebben be is mutatok. Ez csak egy a folyamatosan növekvő számú hasonló esetek közül, ami jól rávilágít arra, hogy az ember egyre kevésbé tudják kontroll alatt tartani a személyes adataikat.

Ilyen környezetben és ilyen események láttán nagy hangsúlyt kell fektetni az adatvédelmi szabályozásokra. Ezt az európai jogalkotók is észrevették, majd a XX. század második felétől fokozatosan létrehozták a személyes adatok kezelésének jogi keretrendszerét. Eme rendszer megalkotásának eddigi talán legnagyobb állomása az úgynevezett általános adatvédelmi rendelet (General Data Protection Regulation , GDPR) létrehozása és bevezetése, amely segítségével létrejött az európai szintű összehangolásaés egyesítése a személyes adatok védelmének. A rendelet 2018. május 25-én lépett érvénybe, két éves türelmi idő után, ami a közélet figyelmének középpontjába állította a személyes adatok védelmét.

Szakdolgozatomban a téma aktualitása mellett szeretném bemutatni azt, hogy a rendelet létrejöttének fontossága vitathatatlan a XXI. században, még ha ez az egyén számára nem is jelenik meg közvetlenül. Ezen kívül áttekintem, hogy milyen módon lehet biztosítani az adatok védelmét. A GDPR szabályainak bemutatásán kívül a múltbéli szabályozások képest az ebben szereplő újításait is ismertetném. Igyekszem rávilágítani arra is, hogy ennek megalkotása rendelkezik előtörténettel is, továbbá a megvalósítást is prezentálnám figyelembe véve az elért eredményeket és a jövőbeli lehetőségeket is.

Ami a szakdolgozatom szerkezeti felépítését illeti, először áttekinteném az adatvédelmi jog fejlődésének történetét, kezdve ezt egészen a II. világháború utáni időkkel. Bemutatom mik a fő céljai a GDPR-nak, milyen változásokat eszközöltek az előző szabályozáshoz képest. Ezután áttekintem, hogy milyen eredményeket ért el a rendelet a megalkotása óta. Az hazai adatvédelmi hatóság adatai alapján szemléltetem, hogy milyen változásokat hozott az adatvédelmi incidensek területén.

Majd ezek után a rendelet megalkotásának okaival folytatom. Szóba kerül majd két nagy adatvédelmi incidens is, az egyik még a GDPR életbe lépése előtti időkből, a másik pedig a közelmúltban történt ügy.

Dolgozatom központi részében bemutatom, hogyan lehet megvalósítani ezeket a szabályozásokat egy weboldal üzemeltetője szempontjából. Végül pedig bemutatom, hogy a társult tagok, illetve a harmadik országok tekintetében, hogyan és milyen szabályoknak megfelelve lehetséges az adattovábbítási folyamatok elvégezni.

Zárásként pedig egy kicsit a jövőbe tekintek, és ismertetem, hogy milyen nehézségek állnak még a rendelet előtt a jövőben.

2. A GDPR ÁTTEKINTÉSE

Szakdolgozatomnak ennek a részében először bemutatom az adatvédelem nemzetközi kialakulásának történetét, kezdve a II. világháború utáni időkkel. Röviden ismertetem, hogy milyen változásokat hoztak az egyes szabályozások az előzőkhez képest. Ezek után röviden a hazai történetet is bemutatom. A GDPR részletesebb bemutatásával, jogszabályba foglaltak és az előző irányelvben szereplő előírások összehasonlításával folytatom. Ezt egy bővebb, részletesebb formában teszem meg. Néhány célját is megemlítem a rendelet létrehozásának, illetve annak folyamatát is szemléltetem. A fejezet utolsó részében, pedig leírom hogy jelenleg hogy áll a rendelet. A megalkotása óta hogyan alakultak az adatvédelmi incidensek számai, illetve gyakorlati példát is hozok ezekre.

2.1 A GDPR gyökerei

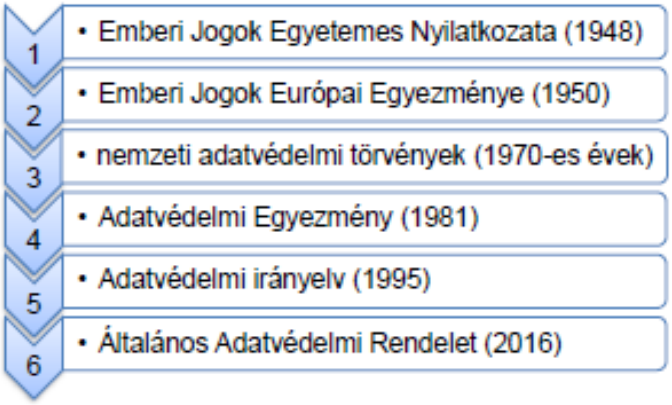
Az emberek személyiségi jogai nagy összefüggésben vannak az általuk betöltött társadalmi szerepükkel. Ezért tehát a társadalmi kondíciók változásával együtt ezeknek jogoknak a megóvásában is újabb körei bukkantak fel. Manapság, a technológia reformjai miatt nagy jelentőséget kaptak ezek a jogok.

A személyes adatok védelme nem túl nagy múlttal rendelkezik az első generációs alapjogokhoz (élethez, szabadsághoz való jog, stb.) képest. A XX. század második felétől beszélhetünk adatvédelmi szabályozásról, mivel a számítástechnika fejlődése miatt innentől volt lehetséges, hogy az egyénekről egyre nagyobb mennyiségű adatot jegyezzenek fel. (SZŐKE, 2014) Az adatok mennyiségének nagy mértékű megnövekedése következtében fontossá vált a személyes adatok védelme.

A kifejezetten rövid múlttal rendelkező adatvédelmi szabályozás ellenére több korszakra tagolható. A korszakok számát tekintve a szakirodalomban nincsen közös álláspont, ugyanakkor legtöbb szerző – köztük Majtényi László (MAJTÉNYI, 2003) is, aki az első ilyen típusú tanulmányt adta ki – három generációt különít el egymástól. 1970-es években jöttek létre az első generációs szabályok, és mivel egyre elterjedtebb lett a számítógépes nyilvántartás, adatbiztonsági korlátozásokat hoztak létre. A második generációs szabályozások, amik az 1980-1990-es években jöttek létre, már nem csak a számítógépes, hanem a papíralapú nyilvántartásokra is vonatkozik, illetve a nemzetközi adattovábbításokra is kiterjedtek az adatvédelmi szabályok. Ennek a korszaknak,

generációnak a része volt az is, hogy a jogalkotó az adatkezelés teljes folyamata közben is jogokat kapott, nemcsak az adatkezelés megkezdése előtt. (MAYER-SCHÖNBERGER, 1997) Az utolsó, harmadik generáció során az adatvédelem európai szintű harmonizálása, továbbá a különféle iparágakra specializálódott adatkezelési-adatvédelmi szabályok megalkotása volt a meghatározó.

Mint azt a bevezetésben is már említettem, a rendelet megalkotása korántsem előzményektől mentes, hiszen a GDPR megalkotásához több európai adatvédelmi szabályozáson át vezetett az út. Ezt szemlélteti következő ábra, amely az előbb említett 3 generációnál jóval korábbról kezdi az áttekintést, hiszen a XX. század közepétől már beszélhetünk adatvédelemről:



1. sz. ábra: A GDPR előtti szabályozások (forrás: saját szerkesztés (www.wikipedia.hu))

Először 1948-ban fogadták el az Emberi Jogok Egyetemes Nyilatkozatát. Innentől kezdve foglalkozik a jog az adatvédelemmel. Természetesen ez még csak nagyon érintőlegesen foglalkozott a témával. Ezt az Egyesült Nemzetek Szervezete (ENSZ) adta ki, amiben nem sok szó esik az adatvédelemről, azonban ezt egy mérföldkőnek tekinthetjük, mivel ezzel jött létre a személyiségi jogok védelmének keretrendszere, alapja.

Ezt vették alapul amikor 1950-ben megalkották az Emberi Jogok Európai Egyezményét az Európai Tanács tagjai. Az egyezményt aláíró országoknak innentől kezdve kötelezettsége volt az emberi jogok tiszteletben tartása.

Az előbb említett két nyilatkozat még nagyon kezdetlegesnek minősült és egyik sem kimondottan a személyes adatok védelmével foglalkozott. A következő évtizedekben azonban ez változott. Az egyre fokozódó technológiai fejlődés következtében lépniük kellett az országoknak is. Erre azért volt szükség, mert a számítástechnika ekkor eljutott

már arra a szintre, hogy elektronikus módon legyen képes az adatokat tárolni és kezelni. Ennek következtében pedig a jogalkotókat foglalkoztatni kezdte ezeknek az adatoknak a védelme, majd így születtek meg az első adatvédelmi törvények nemzeti szinten.

Mindezek után 1981-ben került sor az adatvédelemre koncentráló és kifejezetten csak azzal foglalkozó, európai szintű egyezmény kiadására, ami kötelező erejű. (PÉTERFALVI, 2012) Ez az Európai Tanács által lett elfogadva, amiben az automatizált adatnyilvántartással kapcsolatban próbáltak valamiféle védelmet biztosítani. Azért fontos mérföldkő ez, mert ebben az egyezményben említik először a személyes adatok védelmének jogát, mint a magánélet jogának egyik reprezentálása. (SZIKLAY, 2011) Ezen kívül a különleges adatok nagyobb mértékű védelme és a szankciórendszer megalkotása is figyelmet kapott az egyezmény létrehozóitól. (SZŐKE, 2014) Magyarországon ez az egyezmény 1988 óta a jog része.

Nagyon sokáig ez az egyezmény volt az egyetlen kötelező érvényű, nemzetközi szintű jogforrás, de a technika, a számítógépek rohamos elterjedése, a határon túlnyúló adatmozgások mennyiségének emelkedése, továbbá az adatok továbbítását bonyolító, nemzetenként különböző szabályozások egységesítése egy sokkal alaposabb szabályrendszer megalkotását tette szükségessé. Ennek következtében jött létre egy újabb nagy mérföldkő, az 1995. október 24-én életbe lépő irányelv, a 95/46/EK számú.

Ez az irányelv nagy előrelépést jelentett az adatvédelem területén az Európai Unión belül. Két fontos szempontot tartottak szem előtt mikor létrehozták az irányelvet. Egyrészt, hogy az emberek alapvető jogait megóvják a személyes adatok felhasználása során, másrészt, hogy az EU tagállamai között szabadon áramolhassanak az adatok. Ezt úgy valósították meg, hogy az adatok nagy mértékű óvásával biztosították azok korlátok nélküli mozgását EU-n belül, és azon kívül is. (SZŐKE, 2014) Ez az irányelv nagy mértékű pozitív fejlődést jelentett az előző szabályokhoz viszonyítva, melynek legjelentősebb újdonságai Jay és Hamilton (JAY-HAMILTON, 1999) alapján a következő pontokban összegezhetők:

1. automatizált és manuális adatfeldolgozásra is vonatkozik az irányelv,
2. az adatfeldolgozás törvényességéről szóló előírások írásba foglalása,
3. az érzékeny adatok felhasználására külön szabályok,
4. az érintettek jogainak definiálása,
5. az adatfeldolgozás- és kezelés során szigorúbb adatbiztonsági szabályok,
6. a határon átnyúló adatküldések részletes előírása,
7. adatvédelemmel foglalkozó, 29. cikk szerinti munkacsoport alakítása.

1998-ig minden Európai Unió-s országnak be kellett vezetnie a saját szabályozásaiba, ezáltal valójában ez alkotta meg az egységes, európai szintű adatvédelmi rendelkezés alapjait. (SZŐKE, 2013) Az adatvédelmi irányelv eredményei és hatékonysága elmaradt a tőle elvártaktól, mivel azok az adatfeldolgozó tevékenységek, melyek megengedettek voltak az EU tagjai számára, máshol törvénytelennek minősülhetnek. (VOIGT-VON DEM BUSSCHE, 2017) Illetve az eltelt idő alatt végbement technológiai és társadalmi előrehaladás következtében azonban elkerülhetetlenné vált az adatvédelmi szabályozás teljes szintű újragondolása, melynek köszönhetően elfogadásra került 2016-ban az általános adatvédelmi rendelet (General Data Protection Regulation, GDPR).

Hazánkban az előzőkben leírtakhoz képest, kissé másként alakult az adatvédelem története. Nálunk is a XX. században kezdtek foglalkozni ezzel a témával. Először 1977-ben a Polgári Törvénykönyvben történt korrekció tekinthető az első lépcsőfoknak. Ekkor a törvénybe belekerült, hogy a már elektronikusan végbemenő adatfeldolgozás nem károsíthatja a személyhez kapcsolódó jogokat. Ezen kívül belehelyezték azt is, hogy az érintett jegyzékbe vett adatairól csak olyan személyek vagy szervek kaphat információt, amelyeknek erre megfelelő illetékük van, illetve az érintettek helyesbítési jogot is kaptak, ami annyit jelent, ha az alany a jegyzékbe vett adatait hibásnak találja és nem egyezik meg az igazsággal, akkor élhet ezen jogával, aminek következményeképpen korrigálniuk vagy kiegészíteniük kell a nyilvántartásban szereplő adatokat.

A személyes adatok védelmének alapvető emberi jogát Magyarországon először 1989-ben az Alkotmány módosítása során vezették be.

Hatalmas fejlődésnek számított a személyes adatok védelmének alapvető emberi jogaként történő bevezetése, azonban ez a módosítás még nem tért ki arra részletesen és nem határozta meg a személyes adat védelmének pontos fogalmát. Ennek következtében a jogszabály gyakorlatban való alkalmazása problémákat vetett fel, mivel nem lehetett ennek pontos definícióját tudni, ami által az Alkotmánybíróság elé kerültek ezzel kapcsolatos ügyek. (MAJTÉNYI, 2006) Az Alkotmánybíróság egy határozata megszüntette a jegyzékekről és a személyes adatok használatáról szóló régebbi szabályozásának egy szegmensét azért, mert azok nem tettek eleget a személyes adatok védelméhez való jognak. Ez a rendelkezés nagy mérföldkövet jelentett az adatvédelmi szabályozásban, mivel több olyan személyes adat védelmével összefüggésbe hozható jogintézményt

hozott létre, amelyek mind a mai napig részét képezik az adatvédelmi szabályozásnak. (PÉTERFALVI, 2012)

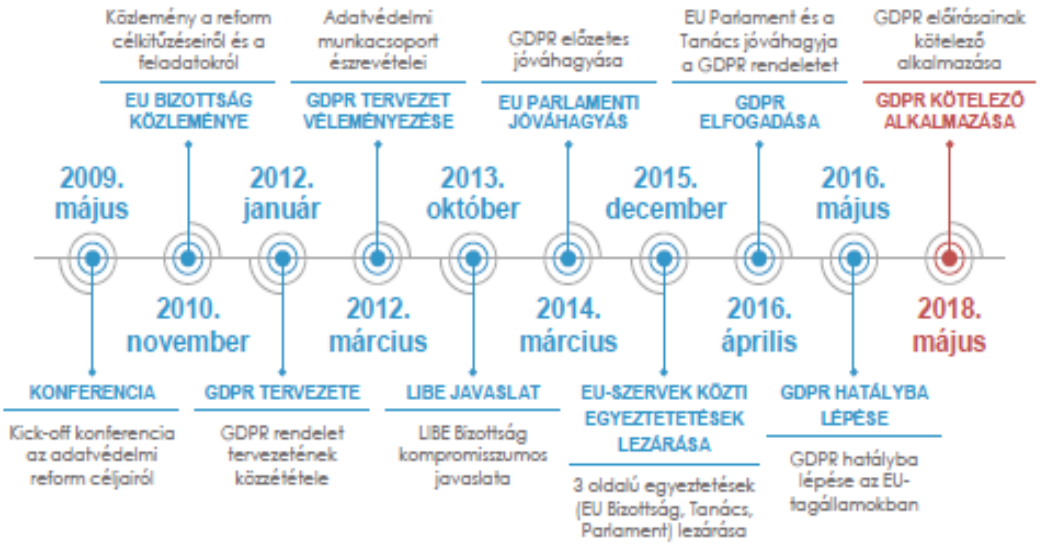
Mindez az előtörténet után 1992-ben került sor egy Országgyűlés általi törvény megalkotására, ami a személyes adatok biztonságáról, illetve a közhasznú adatok nyilvánosságáról szól, és ez a törvény volt országunk első adatvédelmi törvénye. Ezzel Európától eltérően kissé később kezdett fontos lenni az adatvédelem hazánkban, hiszen 1970-ben, az adatvédelmi rendelkezések első korszakában már létrejött a nemzeti adatvédelmi törvény, amit több ország is alkalmazott, azonban Magyarországon már az adatvédelem második korszakának fejlettségét fedezhettük fel az újonnan megalkotott törvényben. Ennek értelmében a törvény már nem csak a manuális, hanem a gépeken történő adatok feldolgozását is érinti. Lényeges lenne még említést tenni arról is, hogy a jogszabály a személyes adatok védelmének alkotmányos jogán kívül a közhasznú adatok nyilvánosságát és az ombudsman létrehozását is megszabta. (JÓRI-HEGEDŰS-KEREKES, 2010)

Az előbb megismert 1992-ben létrehozott törvényt, majdnem húsz évvel később, a 2011-ben elfogadott és életbe lépett Infotörvény cserélte le. Az Infotörvény nagy változást nem hozott a korábbi adatvédelmi rendelkezésben, mert megtartotta annak főbb elemeit, de néhol történtek változtatások, bővítések és helyesbítések a törvény szövegében. Azonban a legjelentősebb újítás egy hivatalos szerv létrehozása volt, az úgynevezett Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH). Ez a hatóság közigazgatási szervként működik. A NAIH váltotta fel az és létrehozásától ő látja el az ombudsman feladatait, továbbá más jogokat is kapott. (PÉTERFALVI, 2012) Az Infotörvény megalkotása óta Magyarországon a személyes adatok védelmét ez a törvény látja el, mióta létrejött a GDPR, azóta annak kibővítésével és korrigálásával továbbra is az Infotörvény van hatályban.

2.2 Mi a GDPR és melyek a fő céljai

Az adatvédelmi irányelv 1995-ben való létrejöttével kisebb-nagyobb sikerrel sikerült Európában egységes, az országok adatvédelmi rendszerét harmonizáló és azokat magasabb szintre emelő adatvédelmi szabályrendszert alkotni. Azóta azonban nagy mértékű fejlődés ment végbe a világban. Az EU a 2000-es évek második felében ébredt arra, hogy az adatvédelmi irányelv már nem képes tartani a tempót a világban végbemenő hatalmas technológiai és társadalmi fejlődéssel, ami új kihívások elé állítja a szabályrendszert. Emiatt volt szükség a szabályozások újragondolására, ami következtében egy teljesen megújult jogszabály, az Általános Adatvédelmi Rendelet (General Data Protection Regulation, GDPR) létrehozatalára tettek javaslatot.

Az új szabályrendszer sok évet igénybe vevő munka eredményeként jött létre:



2.sz. ábra: A rendelet létrejövetelének folyamata (forrás: saját szerkesztés)

Először 2009-ben fogalmazódott meg az európai jogalkotókban egy konferencia során, a korábbi személyes adatok védő szabályozások megreformálása. Ennek a konferenciának a keretein belül már el is kezdődött az új rendszer felépítése. 2010 őszén egy tájékoztató formájában már az Európai Bizottság már ismertette adatvédelemmel kapcsolatos újításoknak a leglényegesebb pontjait. (EURÓPAI BIZOTTSÁG, 2010) Ebben a kiadott tájékoztatóban leírtak között szerepelt, hogy az Európai Unióban egy olyan jogrendszerre van szükség, ami a tagállamokat egységesíti és harmonizálja az adatvédelemmel kapcsolatos szabályozásaik tekintetében, illetve ha céljuk, hogy megvédjék az Uniós állampolgárok személyes adataik védelméhez fűződő jogaikat, mind

az EU-ban, mind pedig azon kívül, akkor változtatásokra lesz szükség a korábbi irányelvben.

Az Európai Bizottság 2012 elején, több éves munka után adta ki a megújított adatvédelmi szabályozást, a GDPR-t (General Data Protection Regulation) (EURÓPAI BIZOTTSÁG, 2012) Az előző irányelvhez képest felfedezhető volt a nyilvánosságra tétel után, hogy nem a korábbi szabályozás módosítása helyett, egy egészen más formát használtak, rendeleti formát. Abból az okból történt így, hogy a rendelet azonnal hatályos legyen minden Európai Uniós tagra és azoknak a jogrendszereikre, vagyis kötelezően implementálniuk kelljen abba, annak érdekében, hogy megszűnjön az országok eltérő szabályozásaikból probléma és létrejöjjön az egységes nemzetközi adatvédelem.

Mivel ez még csak egy tervezet volt, természetesen rengeteg javaslat érkezett, ami által változtatásokat kellett eszközölni a rendeleten. Az Európai Bizottság, az Európai Unió Tanácsa, illetve az Európai Parlament további tárgyalásokat folytatott a rendelet tökéletesítése érdekében, így 2015 végén ők hárman megegyeztek a rendelet végleges leírásában, amit majd 2016 tavaszán az Európai Parlament és az Európai Unió Tanácsa is jóváhagyott.

Amint az az ábrán is látszik, hogy 2016. május 24-én az Európai Parlament és az Európai Tanács a 2016/679 számú rendeletét elfogadta és hatályba is léptette. A GDPR életbe lépésével együtt a 95/46/EK irányelv hatályon kívül lett helyezve. A rendeletben meghatározott új szabályok beiktatására két éves türelmi időt szabtak meg, így az Általános Adatvédelmi Rendelet csak 2018. május 25-től volt a tagállamoknak kötelességük használatba helyezni.

Mióta adatvédelemről beszélhetünk, vitathatatlanul az általános adatvédelmi rendelet a legalaposabb szabályozás. A rendelet minden pontjára kiterjedő elemzése valószínűleg nem férne bele a szakdolgozatomba, így a fontosabb vagy újdonságnak számító részeket emelném ki.

A reform célja az volt, hogy korszerűsítsék az eddig Infotörvény néven ismert szabályozásokat, illetve a büntetőügyekben használt személyes adatok védelméről szóló kerethatározatot. Az új rendelet nagyon megváltoztatta a személyes adatok felhasználására kiterjedő szabályozást és minden hatóságnak, szervezetnek és társaságnak is figyelembe kellett ezt vennie, akik az EU-ban tartózkodók személyes adatait használja és tárolja.

A GDPR bemutatását a tárgyi hatállyal kezdeném. Ezen nem változtattak az előző szabályozáshoz képest, mivel a személyes adatok automatizált és a manuális adatfelhasználás arra a szegmensére is kitér, ami szerint a személyes adatokat nyilvántartási rendszerekben tárolják.

A rendelet megértése érdekében fontos, hogy tisztában legyünk bizonyos alapfogalmakkal. Ezekben nem sok változást hozott a GDPR, hiszen a többsége már az Infotörvényben is megtalálható volt. Csupán néhány apró változtatást, kiegészítést eszközöltek.

Az adatvédelem legjelentősebb fogalma a személyes adat. Ennek meghatározásában nem történt változás, ezt már a korábbi szabályozásban is igen szűkszavúan fogalmazták meg, ami egy nagyon tágan értelmezhető fogalom, miszerint minden információ, ami az érintetthez köthető az személyes adatnak minősül. A személyes adatok mindenki által ismert formái a személyazonosító adatok (név, születéssel kapcsolatos információk, stb.), de ezeken kívül külső tulajdonságok, gazdasági, kulturális, genetikai adatok, illetve az adott személyről készült fénykép vagy hangfelvétel is személyes adatnak minősülhet. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018)

A különösen érzékeny adat esetén azonban már hozott újdonságot a GDPR. Beiktatta például a genetikai- és biometrikus adatot, illetve megtiltotta ezen adatok kezelését, amire csak kivételes esetekben lehet sort keríteni, például ha az érintett engedélyezi azt.

A rendelet az Infotörvényhez képest nem kezeli külön fogalomként adatfeldolgozást és adatkezelést, csak az adatkezelést határozza meg. Ennek alapján az adatkezelés kiterjed minden olyan tevékenységre, amely kapcsán személyes adatokat automatizálva vagy nem automtizálva valamilyen műveletet hajtanak végre azokon. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018) Ha jobban megnézzük, akkor ebben történt változás a korábbi meghatározáshoz képest.

Következő lépésben az alapelvekben bekövetkezett változásokat mutatom be. Ezek az elvek fontos szerepet játszanak, így az új rendelet szövegében is, az előző irányelvben már tapasztalt módon, itt is egy külön bekezdést kaptak, mivel ezek teszik lehetővé, hogy az érintettek élhessenek jogaikkal, illetve ezek teremtik meg az adatok védelmének rendszerét. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018)

A rendeletben szereplő hét alapelv közül öt már korábban is része volt mind az Infotörvénynek, mind az irányelvnek. Ez az öt alapelv a korlátozott tárolhatóság, ami annyit jelent, hogy a érintett adatait, amelyek őt azonosíthatóvá teszik, csak addig lehet tárolni, amíg azok az adatkezelő folyamatokhoz nélkülözhetetlenek. A pontosság elve, miszerint csak pontos és naprakész adatokat lehet használni. Az adattakarékosság, ami kimondja, hogy az adatokat csak a szükséges ideig és a cél elérésének érdekében kellő mértékben való kezelése megengedett. A következő alapelv a célhoz kötöttség, ami megszabja, hogy az adatokat csak meghatározott, egyértelmű és jogszerű céllal történő felhasználása lehetséges. Az utolsó olyan elv, amit már korábban is ismerhettünk a jogszerűség, tisztességes eljárás és átláthatóság alapelve. E szerint az előírásoknak eleget tevő módon csak akkor lehetséges az adatkezelés, ha az érintettet a folyamat megkezdése előtt teljes körűen tájékoztatni kell annak megkezdéséről és az adatkezelés részleteiről.

Az alapelvek között azonban felfedezhetünk némi újdonságot, két új alapelvet fogalmaztak meg: az integritás és bizalmas jelleg elvét, továbbá az elszámoltathatóság elvét. Az előbbi az adatbiztonságra fókuszál. Ez azt jelenti, hogy az adatkezelőnek kötelessége meggátolnia az adatokhoz való jogtalan hozzáférést, károkozást vagy azok elvesztését, mindezt úgy, hogy megteszi a megfelelő lépéseket a biztonságot adatkezelés érdekében. Az adatbiztonság alapelvként való meghatározását az informatikai biztonság egyre nagyobb szerepe tette elkerülhetetlenné, ami a technológiai előrehaladás miatt egyre nagyobb kihívások elé állítja az adatkezelőket. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018)

Az elszámoltathatóság elve nem csak azt foglalja magában, hogy az rendeletben szerepelteket be kell tartania, hanem azt is, hogy adott esetben ezt bizonyítani is tudja. Ez komoly megpróbáltatások elé állítja az adatkezelőt, hiszen informáló anyagokat, belső szabályrendszert kell létrehoznia. Esetleges hatósági ellenőrzés során ezekkel tudja bizonyítani, hogy a rendelet szabályainak megfelel.

Következő pontban a jogalapokról lesz szó. Ahhoz, hogy létrejöhessen a jogszerűség elve, az adatkezelésnek kielégítő jogalapra kell épülnie. Korábban a személyes adatokat kezelni csak az érintett engedélyezésével vagy törvény általi elrendeléssel lehetett, azonban a rendelet sokkal több jogalapot biztosít erre. (JÓRI-SOÓS-BÁRTFAI-HÁRI, 2018)

3.sz. ábra: A GDPR-ban szereplő jogalapok (forrás: saját szerkesztés (www.eur-lex.europa.eu))

Minimum egy jogalapnak eleget kell tenni a fentiek közül ahhoz, hogy szabályos legyen az adatok kezelése. Amennyiben ez nem történik meg, abban az esetben nem lehet az adatkezelő folyamatot elindítani, illetve ha a jogalap már nincs kielégítve, akkor az adatfelhasználást rögtön abba kell hagyni. Abban az esetben, ha az adatfelhasználás nem csak egy jogalap szerint mehet végbe, akkor az adatkezelőnek ki kell jelölnie egyet, mivel ugyan azokat az adatokat nem szabad egyszerre több alapon is használni ugyan abból a célból. Továbbá azért is lényeges, hogy az adatkezelő kijelöljön egy jogalapot, mert mindegyik más-más joggal ruházza fel az érintetteket.

Hazánkban, korábban az Infotörvényben az érintettek hozzájárulását, továbbá azt tartotta a legfontosabb jogalapnak, ha az adatkezelést valamilyen törvény követelte meg. Elkülönített ezeken kívül más jogalapokat, amiket másodlagos jogalapnak nevezett. Ezek voltak a szerződés teljesítése, a jogos érdeknek való megfelelés, illetve bizonyos jog követelmények való eleget tétel. A másodlagos jogalapok használatára csak abban az esetben kerülhetett sor, ha az érintett hozzájárulását valamilyen okból kifolyólag nem lehetett beszerezni, vagy ha az túl nagy mértékű kiadást vont volna maga után. Az álalános adatvédelmi rendeletben is megjelennek ezek, az Infotörvényben is megtalálható jogalapok, de azzal ellentétben a GDPR ezeket azonos szinten kezeli, nem rangorolja őket.

A gyakorlatban ez leginkább az érintett hozzájárulásával történik. (PÉTERFALVI-OSZTOPÁNI, 2017) Az ehhez szüksége feltételek már az Infotörvényben is megtalálhattuk, így a GDPR-ban lényeges eltéréseket ennek tekintetében nem vehetünk észre. Annak ellenére, hogy az érintett általi hozzájárulás a leggyakrabban előforduló jogalap, az adatkezelés lefolytatásához sok esetben használják a szerződés feltételeinek kielégítését, mint szükséges jogalapot. Amennyiben ez a helyzet áll fenn, akkor a rendelet szövege szerint kettő lényeges feltételnek kell eleget tenni. Ezek a feltételek azok, hogy a szerződés egyik résztvevője okvetlenül az érintettnek kell hogy legyen, valamint az adatok felhasználása és a szerződés célja között tárgyilagos viszonynak kell fennállnia. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018) Tehát, ha az interneten megy végbe egy vételezés, akkor szabályosnak minősül az érintett adatainak felhasználása, mivel anélkül nem lehet érvényes egy szerződés, ha a felek személyes adatai nem ismertek és azok nincsenek rögzítve.

Mivel az adatkezelő esetében is vannak bizonyos dolgok és kritériumok amiknek meg kell feleljen, ezért az ezeknek való eleget tétel érdekében is használhatók személyes adatok. Bizonylatolási kötelesség is egy ilyen indoknak tekinthető, továbbá ha pénzmosásra gyanakszik az adatkezelő bizonyos ügyletek alapján, akkor azt muszáj jelentenie. Egy lapon említhetők ezek a közhasznú teendők kielégítésével, illetve a közhatalom gyakorlásának segítésével, ami tulajdonképpen majdnem teljesen azonos az kötelező adatkezeléssel, amely meghatározást a hazai adatvédelmi szabályozásban is fellelhetünk. (JÓRI-SOÓS-BÁRTFAI-HÁRI, 2018) Ezek közé vehetjük a NAV (Nemzeti Adó- és Vámhivatal) által kezelt adóbevallásokat, illetve az előbb említett közhatalmi intézmények adathasználatát is. A való életben ezt a kettő jogalapot viszonylag gyakran alkalmazzák az adatkezelés megkezdése érdekében, az érintett vagy valamely eltérő személy elengedhetetlen érdekeinek megóvása érdekében történő adatkezeléshez képest. Az említett jogalapokat csak olyan esetekben lehet igénybe venni, amikor az érintett testi épségét fenyegeti valami, például egy járvány.

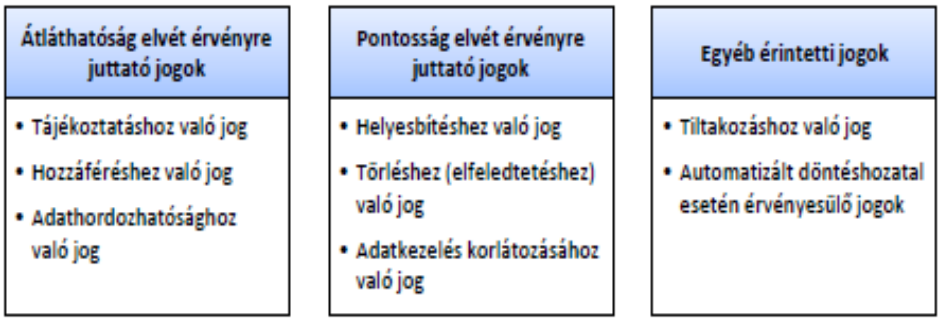
Amennyiben az előzőekben említett öt jogalap egyike sem teljesül, akkor van lehetőség meg egy alkalmazására. Ezt azonban nem sokszor szokták használni. mivel az esetek nagy részében valamelyik jogalapnak eleget tudnak tenni az adatkezelők a tevékenységük elvégzése érdekében. Azonban, ha az adatkezelő az ő maga vagy egy másik személy érdekében jogszerűen hajtana végre adathasználatot, akkor erre hivatkozva a jogalap ezt megengedi. Leggyakrabban olyan esetekben kerül ez elő, mikor videófelvételes felügyeletet alkalmaznak, továbbá mikor a hitelkérelem benyújtása és a

döntéshozatal során az érintettek adatait vizsgálják. Amennyiben ezek közül valamelyik helyzet áll fenn, akkor az adatkezelési folyamat indítása előtt, utána kell járni, hogy a tevékenység valóban jogszerű, nem ütközik az érintett jogaiba és ezt az adatkezelőnek kötelessége tényekkel alá is támasztani. Ezt érdekmérlegelésnek nevezik. Ennek a tesztnek a fejleményéről az érintettet mindenképpen informálni kell, és amennyiben ő úgy dönt, hogy nem szeretné, ha a személyes adatait felhasználnák, ebben az esetben alkalmazhatja a tiltakozáshoz való jogát, amivel megtilthatja az adatkezelést. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018)

Továbbá az is jelentős újításnak számít, hogy a jogszabályi kötelezettségen alapuló vagy közérdekből szükséges adatkezelések esetén, három évente köteles az adatkezelő felülvizsgálni, hogy szükségesek e ezek a folyamatok.

A személyes adatok védelmének egyik legfontosabb része az információs önrendelkezési jog. Ezért lett tehát a rendelet megalkotása során az egyik fő szempont, hogy olyan rendszert hozzanak létre, melyben az egyének önmaguk dönthetnek az személyes adataikról. Az általános adatvédelmi rendelet létrejötte előtt ez csak limitáltan teljesült, ezért a GDPR alkotói nagy hangsúlyt fektettek egyének jogainak kibővítésére, annak érdekében, hogy a gyakorlatban is ők rendelkezhessenek a személyes adataik felett.

Az érintetti jogok kapcsán a már korábban használatban lévő szabályokra alapoztak, azonban vannak újdonságok is köztük:



4.sz. ábra: Az érintett jogai (forrás: saját szerkesztés (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018))

Az átláthatóság elve talán a leglényegesebb az érintettek jogai közül. Ennek értelmében az adatkezelőnek kötelessége informálnia az adatalanyt már a folyamatok elindítása előtt, hogy mit kíván tenni az adatkezelő az érintett személyes adataival. Ez a fajta, érintett irányéba történő informálás, az adatkezelő alapvető és elmulaszthatatlan teendői közé tartozik, ennek automatikus meg kell történnie, annak ellenére is, ha erre az

érintett külön igény nem nyújt be. A rendelet alaposan leírja, hogy a tájékoztatónak milyen kötelező részei vannak (pl. adatkezelés célja, adatkezelő adatai, milyen személyes adatokat használnak, stb.).

Ennek írásos formában kell történnie, legyen az akár a jól megszokott levél formájában, vagy akár számítógépen keresztül. Azonban ha az érintettnek nem felel meg az írásos forma, akkor jogában áll szóban történő értesítést kérnie. Továbbá rövidnek, érthetőnek és bárki számára díjmentesen elérhetőnek kell lennie. Ezeken kívül kötelező a tájékoztatás kiküldését úgy időzíteni, hogy az adatkezelés folyamatának elindulása előtt értesüljön annak lényegi részeivel és céljával az adatalany.

A hozzáféréshez való jog is azt biztosítja, hogy az egyén személyes adatinak kezelésével kapcsolatban kaphat és kérhet tájékoztatást. Az eltérés viszont az, hogy ennek kapcsán bármikor, az adatkezelési folyamat bármely szakaszában kérhet tájékoztatást az adatalany, ehhez semmilyen indoklás nem szükséges. Ezek alapján látható, hogy ha az adatalany a hozzáféréshez való jogát szeretné alkalmazni, akkor ahhoz ennek szándékáról köteles értesíteni az adatkezelőt, neki pedig 30 nap letelte előtt eleget kell tennie ennek a kérésnek.

A GDPR egyik legnagyobb újdonsága az adathordozhatósághoz való jog, ami az előző jog kiegészítése. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018) Ennek értelmében az egyén bármikor kérheti az adatkezelőt, hogy személyes adatait átvehesse, vagy másik adatkezelő számára elküldje. Ez a jog azonban csak akkor vehető igénybe, ha az adatalany ebbe beleegyezett vagy a szerződésben szereplő valamilyen indok ezt megköveteli, illetve ez csak az elektronikus úton történő adatkezelés esetén érvényesíthető.

A pontosság elvét érvényre juttató jogok a gyakorlatban kapnak szerepet. A GDPR-ban hármat sorakoztat fel. Ezek a helyesbítéshez, törléshez és az adatfelhasználás korlátozásához való jogok. A helyesbítés joga az adatok korrigálásánál és kiegészítésénél lép érvénybe. Amennyiben az érintett érvényesíteni kívánja ezen jogát, abban az esetben az adatkezelőnek kötelessége annak eleget tenni, mindezt a olyan rövid időn belül, ami csak lehetséges.

Az adatkezelés során a törléshez való jog az adatalany egyik legfőbb jogosítványa. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018) Annak ellenére, hogy az adattakarékosság elve alapján az adatokat csak az adathasználat céljának teljesülése után kell törölni, az egyén már ennek bekövetkezte előtt is kérheti, hogy töröljék adatait. A rendelet azonban vegyíti egy kicsit az adatalany esetleges törlési kérelmét és az

adatkezelő számára előírt törlést, pedig ezek nem egyeznek meg. Az adatok kezelőjének nem csak akkor muszáj törölnie az adatalany személyes adatait, ha az külön utasítja erre, hanem ha egy jogszabály azt megköveteli tőle.

Az adatalany a törlési jogát a beleegyezésének lemondásával vagy tiltakozási jogát használhatja, a többi helyzetben az adatkezelőnek az adatalany kérése meglétének hiányában is minél előbb meg kell semmisítenie az adatokat. (JÓRI-SOÓS-BÁRTFAI-BUZÁS, 2018) Ezeken túl, az adatalanyok eltávolíttathatják a nevüket a különböző online oldalakról.

Megtévesztő azonban, mivel a törlés nem minden esetben egyezik meg a végleges törléssel, megsemmisítéssel, merthogy az Infotörvényben leírtak alapján a törlés, az adatok beazonosíthatatlanná válását jelenti úgy, hogy az érintett és adatai között többé már ne legyen összeköttetés és lehetetlen legyen visszakereshetőség, hogy kihez tartoznak az információk, így már nem is tekinthetők személyes adatnak. (PÉTERFALVI-RÉVÉSZ-BUZÁS, 2018)

A rendelet az eddig említetteken kívül egyéb jogokat is biztosít, ilyenek a tiltakozáshoz való jog és az automatizált döntéshozatal kapcsán érvénybe lépő jogok. A tiltakozási jog biztosítja az érintett számára, hogy amennyiben van rá indoka, leállíttathatja az adatkezelési folyamatot. Abban az esetben, ha az adatkezelő tudja bizonyítani, hogy az érintett érdekeivel szemben álló, azonban jogos indokok kényszerítik, akkor folytatnia kell a tevékenységet.

Az utolsó adatalany joga, ami a pontosság elvéhez köthető, az adatfelhasználás korlátozására vonatkozó jog. Erre abban az esetben van szükség, mikor az adatalany az előzőekben már bemutatott jogai közül érvényesíteni próbálja az egyiket, tehát ha adatok törlését, módosítását, kiegészítését kérvényezte. (JÓRI-SOÓS-BÁRTFAI, 2018) Az adatalany ezekben a helyzetekben kérheti az adatkezelőt, hogy átmenetileg nem folytassa tevékenységét.

A rendelet az előbbiekben felsorolt és bemutatott jogokon kívül felsorol még kettőt. Ezek a tiltakozáshoz való jog és az automatizált döntéshozatallal kapcsolatban alkalmazható jogok. Mivel a tiltakozáshoz való jog igénybevételével az érintett megsemmisíttetheti vagy korlátozhatja adatainak felhasználását, így ez a jog nagy mértékben hasonlít a korábban már ismertetett jogokhoz. Azonban lényeges megemlíteni, hogy ez a jog csak abban az esetben vehető igénybe, ha ennek a kérésnek jogos indokai vannak, továbbá ha közhasznú célból került sor az adathasználatra. Amennyiben az

adatalany él ezzel a jogával, az adatkezelő csak akkor folytathatja tovább az adatok felhasználását, ha alá tudja támasztani, hogy a tevékenységét valamilyen jogos okból kifolyólag köteles elvégezni, ami által el kell tekinteni az érintett kérelmétől, mert az ő érdekében és megóvásának teljesítéséhez szükséges.

A végső érintetti jog ami szerepel az általános adatvédelmi rendeletben, az automatizált adatfeldolgozás által hozott döntések alóli felmentést biztosító jog. Erre nagy szükség volt a technológiai fejlődések miatt, hiszen manapság rengeteg döntés születik meg úgy, hogy az nem köthető emberi tevékenységhez. Ilyen eset az, mikor hitel felvételre készülünk. Ma már az ehhez kapcsolódó döntési folyamat sem emberek által megy végbe, hanem teljesen automatizálva. Ezért hasznos ez a jog, mert ha az adatalannyal kapcsolatban ilyen formában születik meg egy döntés, akkor kérheti eltörlését, mivel ez nagy mértékben befolyásolhatja az érintett életét. Azonban ez a jog sem alkalmazható minden esetben, kivételt képez, amikor az érintett beleegyezik, vagy ha a kettőjük között köttetett szerződés lebonyolításához ez nélkülözhetetlen.

Az eddigiekben már észrevehettük, hogy az általános adatvédelmi rendelet létrejötte és életbe lépése mennyi változást hozott az adatvédelemben. Ezek a reformok a mindennapi használatban nagy terhet róttak adatkezelők és feldolgozók vállára. Az adatkezelők egyik legfontosabb feladatai közé tartozik, az adatalanyok érintetti jogainak való megfelelés, azonban a GDPR más kötelezettségeket is megemlít az adatkezelőkkel kapcsolatban. Az adatkezelőnek a kötelezettségei elvégzése alatt eleget kell tennie a rendeletben szereplő egyik cikk nézetének, amely kimondja, hogy az adatkezelés lefolyása előtt le kell fektetni az arra vonatkozó adatvédelmi szabályokat, majd a tevékenység teljes ideje alatt azoknak meg is kell felelni.

A rendelet alapján az adatkezelő az egyik legfontosabb részvevője a folyamat szabályos lezajlásának biztosítása terén, mivel vonatkozik rá az elszámolhatóság elve, ami alapján az ő feladata az adatkezelési folyamat szabályosságának betartása, illetve ha szükség van rá, akkor ennek fennállását bizonyítani is tudja. Ahhoz, hogy ez sikerülhessen, az adatkezelőknek kötelességük ennek érdekében jegyzéket vezetniük, amely a lehető legrészletesebben kell hogy kitérjen mindenre, illetve amikor az adatalanyoknak tájékoztatót küldenek ki, akkor is ugyan ezeket kell azoknak tartalmaznia.

Nem árt azonban megjegyezni, hogy az efféle feladatkör nem a GDPR során került elő, hanem már korábban, az irányelv is tartalmazta ezt. Azonban akkoriban ez

nem az adatkezelők dolga volt, hanem a Nemzeti Adatvédelmi és Információszabadság Hatóság feladata, mivel az adatkezelőnek még az adatkezelési folyamat elindulása előtt tájékoztatnia kellett a NAIH-ot, hogy milyen tevékenység elvégzésére készül. Ez a rendelet megszületésével együtt el lett törölve és immár ezek a kötelezettségek az adatkezelőre hárultak.

Az adatkezelők másik lényeges feladata az adatok védelmének biztosítása. A rendelet szövege erre nem tér ki részletesen, annyi követelményt szab meg, hogy az adatkezelőnek és az adatfeldolgozónak muszáj olyan intézkedéseket eszközölnie, amelyek biztonságba helyezik az adatalanyok személyes adatait. Ebben az a pozitívum, hogy az adatkezelőnek ezáltal szabad kezet adnak, hogy milyen módon valósítja ezt meg, annyi a lényeg, hogy végezetül eleget tegyen ennek a kritériumnak.

Ez azonban nem minden, ha az adatkezelő feladatait tekintjük. A rendelet előírja számára azt is, hogy amennyiben szükség van rá, ezeket a követelményeknek a nem betartása, milyen lépéseket követel meg tőle. A rendelet kifejti, hogy mi minősül adatvédelmi incidensnek, amikor az adatok az adatkezelés során valamilyen szabályellenes tevékenység alá esnek, például ha azokat megkárosítják, módosítják vagy ha illetéktelen kezekbe kerül. A GDPR szövege alapján az adatkezelőnek 72 órán belül, az incidens észrevételétől számítva, tájékoztatnia kell a hatóságokat. Mikor a bejelentés megszületik, az adatkezelőnek minden fontos pontját be kell mutatnia az incidensnek, azt hogy előre láthatólag mit okoz majd az incidens, kikre terjed ki, illetve hogy milyen módon kívánja ezt javítani és kezelni. Fontos, hogy az adatkezelő az incidensről is jegyzéket vezessen, hiszen a felügyelet ez alapján tudja ellenőrizni, hogy milyen lépéseket tett meg az adatkezelő a probléma megoldása érdekében. Az olyan incidenseknél, amelyeknél az adatalanyokra nagy veszélyt jelenthetnek a történtek, mindenképpen informálni kell őket róla.

Az adatkezelőnek van azonban még egy feladata, a hatásvizsgálat. Ez fontos lépés még az adatkezelési folyamat megkezdése előtt, hogy az adatkezelő a fontosabb lépéseket és műveleteket, illetve egy esetlegesen bekövetkező incidens során, milyen intézkedéseket kíván tenni. Ezt a vizsgálatot nem kell minden esetben végrehajtani, csak olyankor, mikor feltételezhető, hogy az adatalanyok adatai nagy veszélynek vannak kitéve.

Az eddig ismertetetteken kívül a GDPR-ban szerepel az is, hogy az adatkezelő és adatfeldolgozó köteles egy adatvédelmi tisztviselőt megnevezni, néhány kritérium betartása mellett. Ő azért felelős, hogy az adott vállalaton belül megkönnyítse és

hozzájáruljon az adatvédelmi szabályozások teljesítéséhez. Ezt úgy teszi, hogy először felméri az adott vállalatnál lévő helyzetet a GDPR-nak való megfelelés szempontjából, majd hogy mindenben megfelelő legyen a szervezet működése javaslatokat tesz és segíti az előkészítő munkálatokat.

2.3 Hol tart ma a GDPR?

A GDPR 2016-os elfogadása után 2 éves időtartamot kapott minden ország, vállalat akik az adatkezelésben és adattovábbításban részt vesznek, hogy a rendeletben szereplő kritériumnak eleget tegyenek, azoknak megfelelő változtatásokat eszközöljenek a rendszereiken. Ez alatt a két év alatt rengeteg munka és teher várt az adatkezelőkre, mivel minden alaposan szemügyre kellett venniük, ki kellett elemezniük, ami sok időt, pénz és papírmunkát jelentett számukra. Ezáltal, a hosszúnak tűnő két év mégsem volt kellő mennyiségű és ezt egy 2019-ben készített tanulmány is igazol. (CISCO SYSTEMS, 2019) Több mint háromezer cég részvételével készült el ez a felmérés, ami alapján kiderült, hogy az adatkezelők 59%-a vélte úgy, hogy eleget tesz a rendeletben szereplő szabályoknak. Kiderül még ebből a tanulmányból az is, hogy az adatkezelők véleménye alapján a megfelelő védelmi szint kialakítása, a dolgozók oktatása az adatvédelemmel kapcsolatban, illetve a rendeletben foglaltak folyamatos változásának való megfelelés a legnehezebb feladat az adatvédelmi rendelet bevezetésére való előkészületek során.

Egy másik felmérés alapján, amit az Európai Bizottság készített, a 2018-as évben, a rendelet májusi bevezetésétől számítva majdnem 100.000 panaszt kaptak az adatvédelmi hatóságok.

Ebben az évben történt a Google esete is, ami egy komolyabb incidens volt. Ennek végeredményeképpen a Franciaországban található felügyeleti hatóság (Commission Nationale Informatique & Libertés, CNIL) 50 millió eurós összeggel szankcionálta a szabályok megszegését. Ilyen nagy összegű büntetést azért szabtak ki, mert a vállalat adatokról szóló védelmi szabályzata csak nehezen elérhető volt, illetve nem egy helyen összegyűjtve, hanem többszöri klikkelés után volt csak minden elérhető. Ezen kívül, abban is vétkesnek bizonyult a Google, hogy az egyének számára ajánlott reklámok nem az adatalanyok beleegyezése után történt meg, hanem ez egy standard volt a rendszerükben, ami semmilyen módon nem engedélyezett a rendeletben szereplő szabályok alapján. A nagy mértékű pénzügyi szankció nem csak a szabálysértés típusa

miatt született meg, hanem azért is, mert nem egyszeri, sokkal inkább folytonosnak tekinthető, illetve az érintettek nagyon nagy száma miatt.

Hazánkban a Nemzeti Adatvédelmi és Információszabadság Hatóság elkészítette az ugyan erre az évre vonatkozó elemzéseit. (NAIH, 2019) Ebben a saját tevékenységükről osztottak meg információkat. A beszámoló alapján könnyen kijelenthető, hogy a hatóságnak is többszörösére nőtt a feladatainak száma, hiszen az előző évekhez képest sokkal több ügyön kellett dolgozniuk. Ha megnézzük például az adatvédelmi témájú konzultációs beadványokat, akkor látható, hogy a 2017-es 1.298-hoz képest, a 2018-as 2.409, majdnem kétszer annyi beadványt jelent. Ez is arra mutat rá, hogy a GDPR életbe lépése meglehetősen sok kérdést vet fel az emberekben.

Az új adatvédelmi rendelet életbe lépése után összes 67 hatósági eljárás indult el, melyből 17 hivatalból indult. A többi 50 esetben a leggyakrabban munkahelyi, egészségügyi és banki adatkezeléssel, videófelvételes megfigyeléssel, illetve érintetti jogoknak való nem eleget tétel miatt adtak be kérelmeket. A GDPR életbe lépésének első évében hazánkban mindössze 244 incidens bejelentése érkezett. Ez azt tükrözi, hogy az adatkezelők többségi még nincs tudatában annak, hogy az ilyen esetek bejelentése kötelező.

Az adatvédelmi hatóság adatai alapján a legjelentősebb incidens a rendelet megszegésével kapcsolatban Magyarországon a Demokratikus Koalíció által történt. Ebben az esetben szabták ki a legnagyobb összegű, 11 millió forintos bírságot. Erre azért volt szükség, mert a párt weboldalát egy támadás érte, aminek eredményeképpen több mint 6.000 érintett személyes adatai kerültek bárki által elérhetővé. Mind ezek után a Demokratikus Koalíció párt, a rendeletben szereplő bejelentést nem tette meg, illetve az adatalanyokat sem informálták a történtekről. A nagyon nagy mértékű anyagi szankció annak köszönhető, hogy nagy veszélynek lettek ezáltal kitéve az érintettek.

A rendelet bevezetése a hatóságban is változásokat hozott. Teljesen át kellett szervezni a felépítését, több tevékenységi részre kellett bontani, illetve az elvégzendő munka ugrásszerű megnövekedése miatt a munkaerő bővítésére volt szükség.

A NAIH következő évi, 2019-es beszámolóját is kiadta a hatóság. (NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG, 2020) Ez az év azért másabb az előzőnél, mert itt már a teljes évben érvényben volt a GDPR és annak hatásai már jobban észlelhetők voltak. Ebben az évben 1.738 adatvédelmi vizsgálat indult, ami a 2018-ashoz képest több, mint kétszer annyi. Ezeknek a vizsgálatoknak majdnem a 100%-a panasz által kezdődött. Ebből látszik, hogy a mindennapi ember számára is egyre inkább ismertté

válik a rendelet, és tisztában van azzal, hogy milyen jogai vannak a személyes adatai védelmével kapcsolatban. A hatósági eljárások számának terén is jelentős növekedés észlelhető. Míg 2018-ban ez a szám csak 67 volt, 2019-re ez 276-ra nőtt. Ezeknek döntő többsége az adatvédelmi rendelettel kapcsolatos volt. A 276 esetből 240 kérelem útján indult el. Ebben az évben is szinte ugyan azokkal a témákkal kapcsolatban keresték fel a hatóságot, mint az előzőben. 2019-ben összesen 112.734.000 forintos összegben szabott ki bírságokat a NAIH.

A következő év során szintén nagy mértékű növekedést észlelhettünk. (NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG, 2021) Ebben az éveben, az előzőhöz képest majdnem másfélszer annyi bírság beszedésére volt képes a hatóság, ami 256.411.00 forintot jelentett. Az adatvédelmi vizsgálati ügyek tekintetében 2.400-ra nőtt meg ez a szám 2020-ban, ami háromszor annyi volt, mint 2018-ban. Tavalyi év során az adatvédelmi hatósági eljárások ügyeinek száma is megnőtt, 347-re. Ezeknek továbbra is a többsége kérelem volt. 2018-ban 244, 2019-ben 506, és 2020-ban már 781 volt bejelentett incidensek száma. Ami jól tükrözi azt, hogy az adatkezelők is egyre inkább tisztában vannak azzal, hogy kötelességük ezeket az esetek bejelenteniük.

Ezek közül az incidensek közül a DIGI ügy az, amit érdemes megemlíteni, ugyanis 100 millió forint összegű bírságot szabott ki rájuk a NAIH, amire eddig hazánkban még nem volt példa. Ez több mint háromszor akkora összeg, mint amit eddig a hatóság alkalmazott szankcióként. Azért jártak el ilyen szigorúan, mivel egy olyan probléma merült fel, egy hiányosságra került sor, amire már régóta van megoldás, de ennek javítását az adatkezelő nem végezte el. Továbbá nagyon nagy mennyiségű adat került bárki által elérhetővé, ezáltal nagy kockázatnak kitéve az érintetteket, illetve a rendeletben alapelvként meghatározott kritériumnak sem tettek eleget ezért volt szükség a nagyobb mértékű szankció használatára is.

3. A KIVÁLTÓ OKOK

Ebben a fejezetben az általános adatvédelmi rendelet megalkotásának lehetséges okait mutatnám be. Az indokok között megemlítek egy jogesetet, amely egy kivételes eset volt a magyar jog történetében, mivel hazánk jogszabályait, akkor először alkalmazták egy másik országba bejegyzett vállalaton.

3.1 Figyelmeztető jelek a világgazdaságban

Dolgozatom ezen részében a GDPR megalkotásának valószínűsíthető okait mutatom be. A világban végbe menő ugrásszerű technológiai és társadalmi fejlődés okozta új problémák megoldására hozták létre. Azért volt erre szükség, mert hirtelen megnövekedett az emberekről összegyűjthető személyes adatok mennyisége, amelyek által nagy kockázatoknak voltak kitéve az adatalanyok. Ezt mindenképpen orvosolni kellett, hiszen személyes adataink által befolyásolni és akár megváltoztatni is tudják az életünket. Másik oka a rendelet létrehozásának az lehetett, hogy az előző irányelvek és szabályozások nem kötelező érvényűek voltak. Ebből fakadóan minden ország másként implementálta a jogrendszerébe a szabályokat, így nem volt egyszerű elbírálni az adatvédelmi incidenseket. Másrészt, így minden ország más volt a szigorúsági szinttel rendelkezett az adatvédelemmel kapcsolatban, amit bizonyos cégek ki is használtak.

Ezt a jelenséget hívták forum shoppingnak, aminek a lényege az volt, hogy a korábbi irányelv nem kötelező jellegét, és az országok különböző adatvédelmi jogrendszerét kihasználva jutott előnyhöz néhány vállalat. A különbségekből adódóan voltak olyan országok, ahol kevésbé szankcionálták keményen a szabályok megszegését, volt ahol sokkal kevesebb előzetes óvintézkedést kellett megtenni az adatok védelméért és voltak ahol az adófizetés körülményei is kedvezőbbek voltak. Így minden vállalatok oda telepedett le, ahol az ő tevékenységének elvégzéséhez a legkedvezőbbek voltak a feltételek. A forum shopping megszüntetése volt az egyik oka a területi hatály szigorú kritériumainak megalkotására. A rendeletben szereplő szabályok szerint ugyanis, nem az számít, hogy hol történi meg az adatkezelés, hanem az, hogy kinek az adatait kezelik, és hogy ő éppen ez idő alatt hol tartózkodik.

Hazánkban már 2015-ben volt rá precedens, hogy egy másik országban lehetett alkalmazni a magyar jogszabályokat. Akkoriban ez még nem teljesülhetett volna, azonban egy per során ilyen döntés született. Ez a Weltimmo ügy volt. A Weltimmo egy Szlovákiában bejegyzett cég volt, amely a Magyarországon megtalálható ingatlanokat hirdette az interneten. A szolgáltatásaik igénybe vételének első hónapja még ingyenes volt, azonban onnantól díjköteles. Az ellenük irányuló adatvédelmi eljárás indításának oka az volt, hogy a szolgáltatás lemondása után sem kerültek eltörlésre az érintettek adatai, illetve a költségek is ki lettek számlázva, amik a szolgáltatás lemondása miatt nem is jöttek létre.

Az eljárást a NAIH indította el, majd a bíróság ítélete alapján közel 10 millió forintos pénzbírságot szabtak ki a vállalatra. Ezt a döntést a cég megtámadta, annak okán, hogy nem lehet a magyar jogszabályokat egy másik országban alkalmazni, illetve a NAIH joghatóságát is kérdőre vonták. Az EUB az ítélet során kihangsúlyozta, hogy megnehezítette volna az érintettek jogainak érvényesítését, ha szigorúan nézik azt, hogy a vállalat tevékenysége csak arra az országra terjed ki, ahol le van telepedve. Azért születhetett meg ez a döntés, mert a vállalat tevékenységét Magyarországon is végrehajtotta, a hazánkban található ingatlanokat hirdette, illetve magyar nyelven is elérhető volt az oldal.

Ez volt tehát hazánkban az első olyan eset, mikor hazánk jogszabályait egy másik ország vállalatával szemben is érvényesíteni lehetett.

Egy feltételezhető további magyarázat arra, hogy miért hozták létre az európai jogalkotók az általános adatvédelmi rendeletet, az lehetett, hogy egy egységes és harmonizált európai szintű adatvédelmi szabályozást hozzanak létre, amivel egy zárt közösséget alkotnak meg az Európai Unión belül. Ezáltal rá lesz szorulva a többi ország és vállalat arra, hogy ők is megfeleljenek az GDPR-ban szereplő rendelkezéseknek, hiszen a világ adatainak egy nagy része az Európából származik és a technológiai fejlődés érdekében fontos, hogy az ő adataik is elérhetőek legyenek.

3.2 Személyes adat, mint árucikk

Napjaink információs társdalamában nagy szerepet játszanak az adatok. A személyes adatai által könnyen befolyásolható, irányítható és megváltoztatható egy ember élete. Technológiai fejlődésnek is egy hatalmas rész, a nagy mennyiségű adatok felhasználása azért, hogy fel tudják térképezni az emberek szokásait és azokhoz igazítsanak bizonyos szolgáltatásokat és termékeket.

Ennek szemléltetésére az egyik példa, amit szeretnék bemutatni a Cambridge Analyticához fűződik. Ez az ügy 2016-ban, még a GDPR életbe lépése előtti időkben történt. Közel 87 millió Facebook felhasználó adatait gyűjtötték össze és használták fel politikai célokra. Sokan ezt a botránytartják a 2016-os amerikai elnökválasztáson Donald Trump elsöprő győzelmének okát.

Ez az ügy egészen 2013-ig vezethető vissza, amikor ugyanis Trump tanácsadója megbízta a Cambridge Analyticát, hogy készítsen egy olyan programot, amely képes

azonosítani a szavazókat és adott esetben akár befolyásolni is őket. Ennek a programnak a megalkotásához nem volt elegendő csupán a nagy mértékű pénzügyi támogatás, szükség volt nagy mennyiségű adatra is az emberekről, hogy profilozni lehessen, ki lehessen értékelni a viselkedésüket, véleményüket, ami által könnyeben befolyásolhatóvá válnak. Mivel ez a nagy mennyiségű adat nem állt rendelkezésére a vállalatnak, így azokat a Facebookon keresztül szerezték be. Ezt úgy tudták megoldani, hogy egy alkalmazást használtak, ami engedélyt kért a Facebookon keresztül az adatok begyűjtésére. Ez nagy előrelépés volt az ügyben, mivel rengeteg adathoz jutottak hozzá az applikáció segítségével. Minden személyes adatot, azt hogy a felhasználók milyen tartalmakat kedveltek, miket tettek közzé, sőt néhány esetben még magánbeszélgetésekhez is hozzá tudtak férni. Ezen kívül az érintettek ismerősi körétől is meg tudták szerezni az adatokat, akik természetes erről nem tudtak, hiszen tőlük már nem kért engedélyt az alkalmazás.

Ennek a hatalmas mennyiségű adatnak köszönhetően már el tudták végezni a profilozást, amely során rengeteg következtetésre jutottak. Megtudták, hogy milyen típusú és mennyiségű információt kell megosztani ahhoz, hogy az emberek véleménye megváltozzon egy bizonyos témával kapcsolatban. Ezt a tudást használták fel a választások idején, azért hogy Trumpot jobb színben tüntesse fel, ellenfeleit pedig lejárassa.

Az eset után a Facebook nem vállalta a felelősséget az üggyel kapcsolatban, mivel ők az adatok alkalmazáson belüli gyűjtéséhez járultak csak hozzá, állításuk szerint arról nem is tudtak, hogy utána azokkal az adatokkal mik a céljuk. Elismerték azonban azt, hogy 2015-ben észrevették az adatok nem jogszerű használatát, ami után értesítettek minden céget, akik ebben részt vettek, hogy minden adatot töröljenek, amihez nem szabályszerűen jutottak hozzá. Ennek azonban nem tettek eleget a vállalatok.

Ebből látszik tehát, hogy mekkora hatalom kerül annak az embernek a kezébe, aki nagy mennyiségű adatot birtokol az emberekről. Az üggyel kapcsolatban nem csak a Cambridge Analyticát vonták felelősségre, hanem a Facebookot is megbüntették, mert nem volt megfelelő az adatvédelmi rendszerük, ami nagyon kritikus az ő esetükben, hiszen az egész oldal a személyes adatokra épül.

A másik adatvédelmi incidens már bőven a GDPR létrejötte után következett be, pontosabban a tavalyi év során, 2020-ban. Ez az ügy azért érdekes, mivel egy világcégről van szó, illetve ennek az ügynek a kapcsán szabták ki a tavalyi év legmagasabb bírságát, közel 12,5 milliárd forint összegben.

A H&M ruházati cég és márka volt ennek a rendkívül magas bírságnak az elszenvedője. Az ügy során kiderült, hogy az egyik német központjában 2014 óta gyűjtenek adatokat az alkalmazottakról. Ezek között az adatok között szerepeltek orvosi kezelésekről és azok eredményeikről szóló adatokról, amiket mindig megkérdeztek a munkavállalóktól, mikor a betegszabadság után visszatértek dolgozni, ha nyaralásra használták fel a szabadságukat, akkor arról is rögzítették az általuk elmondott élménybeszámolót, ezeken kívül pedig magéleti információkat is tartalmazott, például a családi állapotról vagy a vallási meggyőződésükről. Az utóbbiakat közösségi beszélgetések alapján nyomozták le. Ez mind természetesen nem felel meg a GDPR előírásainak. A jogtalan adatgyűjtésre és használatra akkor került sor, mikor egy technikai hiba miatt már nem csak a vezetők, hanem bárki hozzáférhetett ezekhez az adatokhoz.

Az ügy kapcsán a német hatóságok rengeteg változtatásra kötelezték a vállalatot, annak érdekében, hogy még egyszer ilyenre ne kerülhessen sor, illetve hogy az adatvédelmi rendszerük megfeleljen a rendelet szabályinak. Az ügy lezárása után a H&M nem csak bocsánatot kért munkavállalóitól, de kártérítést is fizetett számukra.

4. A MEGVALÓSÍTÁS

Ennek a fejezetnek a keretein belül mutatom be, hogy az adatkezelőknek milyen lépéseket kellett megtenni, hogy megfeleljenek a GDPR szabályozásának. Egy példán keresztül szemléltetem ezt, ami egy weboldal esetén ismerteti a megfelelő lépéseket. Ezen kívül bemutatom az adatvédelmi hatóságokat. Milyen feladataik vannak, milyen hatáskörökben járhatnak el, illetve az általuk kiszabható bírságokról is írok.

4.1 Felmérés és előkészítés

Az adatvédelmi rendelet bevezetése az adatkezelők és adatfelhasználók számára is nagy fejtörést okozott. A vállalat működését és az adatvédelemmel kapcsolatos szabályozásaikat alaposan át kellett nézni, illetve megoldásokat találni az esetleg hibákra. Ez nagyon sok időbe, pénzbe és adminisztrációs munkába került. Dolgozatomnak ebben a részében sorban végig megyek a pontokon, hogy milyen változtatásokat kellett eszközölniük egy internetes oldal esetén.

Először is változás történt a korábbi irányelvhez képest abban, hogy a rendelet életbe lépése óta már nem kell az adatvédelmi hatóság felé jelezni, amikor egy adatkezelői

folyamat megkezdődik. Azonban olyan bejelentési kötelezettségi keletkezett az adatkezelőknek, hogy amennyiben egy adatvédelmi incidenst észleltek, akkor azt már jelenteniük kell a felügyeleti hatóság felé. Ezt 72 órán belül meg kell tenniük. Ilyen incidens lehet ha feltörik az oldalt és az érintettek adatai bárki számára elérhetővé válnak. Ezért nagyon fontos, hogy például az olyan weboldalak, amelyik CMS rendszert (Content Management System) használnak, minden az elérhető legújabb verziójú szoftvert alkalmazzák, mert a régi rendszereket már nagyon könnyen fel lehet törni.

Következő lépésben az adatkezelőknek el kell készíteniük az adatvédelemről szóló tájékoztatókat, amiket még az adatkezelési folyamat megkezdése előtt el kell juttatniuk az érintettek számára. Ennek a tájékoztatónak tartalmaznia kell, hogy a weboldal adatkezelői mennyi idő elteltével törlik a kezelt adatokat, illetve magáról az adatkezelés folyamatáról is írniuk kell egy részletesebb beszámolót. Ezeken kívül szerepelnie kell benne annak, hogy milyen típusú adatok használnak fel, a cookie-król is tájékoztatniuk kell az érintetteket, illetve azt is meg kell benne nevezniük, hogy kik és milyen vállalatok töltik be az adatfeldolgozó szerepét. Manapság már rengeteg helyen találhatunk ilyen adatvédelmi tájékoztatókra mintákat, de mivel ezek létrehozása nagy odafigyelést és hozzáértést igényel, így érdemes ezt szakemberekre bízni.

Az eddigiekben megismertek alapján már tudni lehet, hogy amikor az érintettek e-mail címeit összegyűjtik, akkor ez a tevékenység is adatkezelésnek minősül a rendelet szerint. Hírlevelek küldéséhez az e-mail címekre szükség van. Ahhoz, hogy hírlapokan tudjon küldeni a felhasználói részére egy weboldal, erről is tájékoztatást kell írni, illetve a hírlevélre történő feliratkozásnak minden esetben önkéntesnek kell lennie. Ezek során is sok fontos szempontnak kell megfelelni, hogy szabályosan a történjen a hírlevelek küldése.

Nagyon elterjedtté váltak a weblapokon az úgynevezett kapcsolat-felvételi űrlapok. Ezeket leggyakrabban arra szokták használni, hogy a weboldalt meglátogatók felvehessék a kapcsolatot az üzemeltetőkkel. Ezekkel az űrlapokkal kapcsolatban is az a dolga az adatkezelőnek, ha meg szeretne felelni a GDPR szabályainak, hogy az űrlap használata során összegyűjtött adatok használatáról pontosan informálja az érintetteket az adatvédelmi tájékoztatóban. Ahhoz, hogy könnyen kezelhető legyen a felhasználók számára, érdemes két jelölő dobozt tenni a tájékoztatóba, hogy azok bejelölésével egyértelműsíthesse, hogy engedélyezi az adatai kezelését. Az egyik jelölő szolgálná azt a cél, hogy a felhasználó tudomásul vette a tájékoztatóban leírtakat, a másikkal pedig beleegyezhetne az adatkezelésbe.

Ha webáruházakról beszélünk, akkor a rendelés leadása során is bőven akad dolga az adatkezelőnek. Ahogyan azt már megszokhattuk, itt is szükség lesz egy tájékoztatóra, amiben kitér az adatkezelő minden olyan részletre, amire eddig is ki kellett. Amikor a vásárló rendelést ad le, előtte újra el kell fogadtatni vele az adatvédelmi szabályzatot. Ennek során is szükség lesz az adatok kezeléséhez az érintettek beleegyezésére. Fontos részlet lehet az is, hogy még a rendelés leadása előtt tájékoztatva legyen a felhasználó, hogy ez egy fizetési kötelezettséget von maga után. Az adatkezelőnek célszerű a rendelés leadásának során is jelölőke használni, annak érdekében, hogy minél több adathoz jusson hozzá. Lényeges azonban, hogy ezek előre nem lehetnek kitöltve. Három különböző jelölőt érdemes használni. Az egyiket az adatvédelmi szabályzat elfogadására, ami ha nem történik meg, akkor meg kell szakítani a rendelést, egy másikat a hírlevélre való feliratkozás érdekében, illetve egy utolsót, ami az adatok kezelését engedélyezi. Akkor sem mehet végbe a rendelést, ha ezt az utolsó jelölőt nem fogadjuk el.

A cookie-k tekintetében is újításokra volt szükség. A rendelet megalkotás előtt is már kötelező volt az oldalra látogatókat tájékoztatni arról, hogy cookie-kat használ a weboldal. Azonban a GDPR meghatározta, hogy a cookie-król az adatvédelmi tájékoztatóban is részletesen be kell számolni az adatkezelő folyamatokról. Továbbá olyan opciót is az érintettnek fel kell kínálni, hogy ha nem szeretnék, nem kell elfogadniuk az összes cookie-t. Abban az esetben, ha egy weboldal marketing cookie-kat alkalmaz, akkor az oldalra való látogatás első alkalmával kérni kell az érintettek beleegyezését ezek használatához, de arra is lehetőséget kell adnunk nekik, hogy ha szeretnék, beleegyezésüket visszavonhatják.

A GDPR egyik nagyon lényeges része az adattakarékosság, ami természetesen a weboldalakra is érvényes. Nem lehet olyan, adatokat kérni az érintettektől, amik nem nélkülözhetők az adott folyamatok elvégzéséhez. Ilyen lehet például egy vásárlás során az érintett életkora vagy neme.

Láthatjuk tehát, hogy nincsen egyszerű dolguk az adatkezelőknek. Rengeteg részlet van, amire oda kell figyelniük, annak érdekében, hogy az általuk végzett munka megfeleljen a rendeletben szereplő szabályoknak.

4.2 Ellenőrző szervek, szankciók

Az általános adatvédelmi rendelet a felügyeleti hatóságoknak is alaposan meghatározza a jogkörét, ezáltal nagy mértékű befolyással van rájuk. Az egyes országok

felügyeleti hatóságainak meghatározása már az irányelvben is szerepelt, azonban az abban leírt kikötések különböző módon történő implementálás miatt a hatóságok jogköre is keveredett és fedték egymást. A GDPR megalkotás által, azonban ezt sikerült tisztázni, hiszen mindenre külön kitér, amit kötelezően alkalmaznia kellett mindenkinek. Ennek eredményeképpen harmonizálták Európa szinten a felügyeleti hatóság jogköreit, illetve megkönnyítette az ellenőrzési folyamatokat.

A GDPR meghatározza a nemzetközi hatóságok egymással való kooperációkat, a teendőket, illetve hogy melyik hatóság milyen ügyekben járhat el. Ezek a hatóságok közhatalmi intézmények, az ő feladatuk az, hogy az érintettek személyes adataikhoz fűződő jogaikat biztosítsák és megóvják. A GDPR szövegében meghatározásra került ezeknek a hatóságoknak a hatáskörei és ezeket kategóriákba is sorolták. Ezek a vizsgálati, korrekciós, illetve az engedélyezési és tanácsadási hatáskör. A vizsgálati hatáskör során a hatóság ellenőrzéseket tart, amely során megvizsgálja, hogy az adatkezelő az rendeletben előírtaknak megfelelően végzi tevékenységét. Amennyiben az adatok védelmével kapcsolatban a szabályok megszegése történt, akkor kerül elő a hatóságok korrekciós hatásköre, aminek során az adatkezelőt értesítheti és felszólíthatja, visszatarthatja az adatkezelési folyamatot és akár bírságot is meghatározhat a részére. Majd az utolsó hatáskör, a tanácsadási hatáskör kerül elő, melynek segítségével az adatkezelőt tanácsadásban részesítheti, vagy az adatok felhasználásába is beleegyezhet.

A rendelet létre hozói nagy hangsúlyt fektettek a nemzetközi hatóságok egymással való összedolgozásuk koordinálására, mivel manapság egyre inkább válnak fontossá az adatok, ezáltal a harmadik országokban megtalálható személyes adatok is. Az olyan esetekben mikor már a határokon túl kell egy bizonyos ügyben fellépni, olyankor a hatóságoknak egymást segítve kell összedolgozni. Amennyiben ez a helyzet áll fenn, akkor a meg kell határozni egy fő felügyeleti hatóságot. Az érintett adatkezelő ezzel a hatósággal áll közvetlen kapcsolatban és rajta keresztül kerülnek intézésre az ügyekre. A rendeletben szereplő kikötés alapján azt a pozíciót az a hatóság kapja meg, amelyik az adatkezelő tevékenységének központjában van. Ez a kijelölt fő felügyeleti hatóság irányíthatja a több ország hatóságai közötti munkát, akik viszont továbbíthatják meglátásaikat a fő felügyelet döntéséről.

A nemzeti felügyeleti hatóságok nagyon fontosak annak segítésében, hogy a rendeletben leírtak teljesülhessenek, illetve a személyes adatok megfelelő mértékben óvva legyenek. A GDPR létre is hozott egy ilyen szervet, az Európai Adatvédelmi Testületet (European Data Protection Board, EDPB). Ez a nemzetközi testület a az

Európai Unió országaiban lévő hatóságoknak a vezetőiből tevődik össze. Ennek a szervnek az a feladata, hogy a rendeletben szereplő szabályokat az EU-n belüli alkalmazását támogassa, és felkarolja azokat akiknek gondot okoz azok betartása.

Ha az adatalanyok a személyes adataik használatával kapcsolatban szabályellenes tevékenység lépett fel, akkor ennek orvoslásáért a felügyeleti hatóságok a felelősek. Amint azt az előbb már ismertettem, a hatóságoknak hatalmukban áll a korrekciós hatáskörüket használva az adatkezelőkkel szemben bizonyos lépeseket megtenni. Az általuk meghatározható szankciók közül a bírságoláshoz való joguk kavarta fel leginkább a port az emberek között, azonban ez a hatáskör a rendelet egyik leglényegesebb fejlesztése. A korábbi irányelvvel szemben, a GDPR tartalmazza azt is, hogy ez a bírság mekkora mértékű lehet legfeljebb. Ha a hatóság úgy véli, hogy nagyon komoly rendelet szegés történt, akkor a szankció mértéke elérheti akár a 20 millió eurós összeget is, vagy akár a megelőző év világpiaci forgalmának 4%-át. Ezek közül azt kell kiszabni, amelyiknek nagyobb az értéke. Ezért tehát az eddig megszokott maximális 20 millió forintos szankciónál ez egy sokkal számottevőbb érték, amit az adatkezelők kötelesek megtéríteni.

A rendelet azt is kimondja, hogy bíróság elé is lehet vinni az ilyen jogellenes tevékenységekről szóló ügyeket. Ha az érintettekkel kapcsolatos adatkezelés jogellenesen történt meg, akkor az adatkezelő ellen jogvitát indíthat. Amennyiben ezt a panaszt helytállónak vélik, és az valamilyen módon ártott az adatalanynak, abban az esetben a bíróság az adatkezelő vagy adatfelhasználó részére pénzbeli jóvátételt szabhat ki. Nem csak az adatkezelő ellen lehet pert indítani, hanem a hatóságokat is bírósági folyamat alá lehet helyezni, amennyiben az adatalany vagy az adatkezelő nem ért egyet a hatóság ítéletével, valamilyen jogos indokból.

5. BELÜL VAGY KÍVÜL?

Dolgozatom ezen fejezetében ismertetem a rendelet által megszabott területi hatályt, ami meghatározza az egyes országok illetve vállalatok számára, hogy rájuk miként vonatkozik a GDPR. Ezt egy ábra segítségével szemléltetem majd, ami könnyíti a megértését. Az Európai Unió tagállamainak és társult tagjainak könnyített helyzetét, az Egyesült Királyság Európai Unióból való kiválása okozta kérdéseket, illetve a harmadik országok lehetőségeit, arra nézve, hogy milyen lépéseket tehetnek meg annak érdekében,

hogy az új rendelet ellenére is részt vehessenek az adattovábbításban és adatkezelésben. Továbbá bemutatom azt is, mit tehet egy vállalat, ha olyan országban végzi tevékenységét, amely nem felel meg az általános adatvédelmi rendeletnek, akkor mit tud tenni, ha mind ezek ellenére adatkezelést szeretne végrehajtani egy EU-n belül tartózkodó adatalannyal.

5.1 Az egyes tagállamok, társult tagok esete

A technológia rohamléptékű fejlődése, továbbá a globalizáció ébresztette arra az európai jogalkotókat, hogy újra kell gondolniuk az európai szintű adatvédelem szabályozását, nem csak azért, hogy az egyének személyes adatait megfelelő módon tudják védeni az egyre növekvő mennyiségű veszéllyel szemben, hiszen egyre nagyobb mértékben hozzák nyilvánosságra, osztják meg személyes adataikat az interneten, ami által a modern technológiáknak köszönhetően nagyon könnyen összegyűjthetők és felhasználhatók lettek azok hanem, hogy egy egységes digitális piacot tudjanak kialakítani, aminek nélkülözhetetlen része volt, hogy szabadon áramolhassanak az adatok a tagállamok között. Ezt a szabad áramlást azonban korlátozni kellett az egyének személyes adataik védelmében. Ennek eredményeként jött létre a GDPR. Mivel ez az Európai Unió minden tagállamára kötelező érvényű lett, ezért a megfelelő változtatások elvégzése után, ezek között az országok között létrejött az adatok szabad áramlása. Azonban az EU-n kívüli országoknak is változtatniuk kellett az adatvédelmi szabályzataikon ahhoz, hogy ők is élvezhessék a rendelet előnyeit.

A rendelet megalkotása előtt az országhatárok, mennyiségi korlátok és a távolság volt a személyes adatok áramlásának feltétele, azonban létrejötte után már a különböző jogrendszerek szabnak csak ennek határt. Az Adatvédelmi Irányelv által létrehozott harmonizált jogrendszer ellenére is különbözőek voltak az egyes országok szabályozásai az Európai Unión belül és kívül is. Ennek következtében alakult ki akkoriban az úgynevezett forum shopping jelensége, aminek a lényege az volt, hogy az egyes vállalatok olyan országot választottak székhelyükül, ahol számukra kedvezőbbek voltak a feltételek a tevékenységük elvégzésére az ottani adatvédelmi szabályozások tekintetében és ezzel a lehetőséggel sokan vissza is éltek.

Ebben fejlődést az Európai Bíróság döntése hozta a Weltimmo társaság ügyével kapcsolatban, ami egy szlovák székhelyű cég. Ennek értelmében már nem csak

Magyarországok végzett tevékenység esetén hanem, akkor is alkalmazható a magyar szabályozás, ha hazai érintettekre irányul az adott társaság tevékenysége.

Magyarország a GDPR megalkotása során úgy vélte, hogy a rendelet megalkotásával a multicégek ellen kell fellépni, méghozzá úgy, hogy kihasználják az egyes országok közötti eltérést az jogrendszerükre tekintve, aminek segítségével meg tudják gátolni a forum shoppingot.

Ilyen előzmények után 2016. május 24-én hatályba lépett General Data Protection Regulation két éves türelmi idő után 2018. május 25-én lépett életbe. Ezalatt a két év alatt minden Európai Uniós tagállamnak és társult tagnak implementálnia kellett az új rendelet szabályozását a saját jogrendszerükbe. Ez vonatkozott az összes EGT (Európai Gazdasági Térség) államra, amik az Unió tagállamaiból, illetve Izland, Lichtenstein és Norvégiából tevődött össze. Ennek értelmében tehát, ha nem az előbb említett országok egyikébe szeretnénk adatot továbbítani, akkor a harmadik országbeli adattovábbítás előírásait kell figyelembe venni. Ezt egy kicsit később fejtem majd ki.

Tagállamok és társult tagok esetén nem korlátozható vagy tiltható a személyes adatok szabad áramlása, mivel a rendelet életbe lépéséig nekik eleget kellett tenniük a benne foglalt szabályozásoknak, tehát nekik nincsen további teendőjük az egymás között történő adattovábbítás során.

5.2 EU szabály, de nem csak az EU számára

Mint ahogy azt már említettem korábban, attól még, hogy a szabályozás az EU tagállamai között köttetett, még a tagállamokon kívüli országokra is vonatkozhat. Ahhoz, hogy az előző pontban leírtakat konkretizálhassuk, előbb meg kell vizsgálnunk a rendeletben szereplő területi hatályt. Ezt, a tárgyi hatályhoz képest, ami igen könnyen megérthető és átlátható, már komplikáltabban fogalmaztak meg.

A rendelet szövegében a 3. cikk alatt találhatjuk meg, hogy milyen esetekben esik a személyes adatok kezelése a GDPR területi hatálya alá. Egyik pontja nem hozott újítást az adatvédelmi irányelvhez képest, miszerint nem kell figyelembe venni, hogy az adatkezelő folyamatok valójában hol mennek végbe, hanem azoknak tevékenységi helye lényeges.

A cikk második pontjában azonban már találkozunk újdonsággal. Ez olyan adatkezelőkre és adatfeldolgozókra vonatkozik, akiknek a tevékenységi helye nem az EU-ban található és olyan adatokat kezelnek akinek az alanya az Unióban van.

Amennyiben valamilyen terméket vagy szolgáltatást kíván nyújtani az előbb említett érintettek számára, attól függetlenül, hogy valóban történik e köztük valamilyen üzletkötés, akkor is alkalmazni kell az rendeletet. Ez annyit jelent, hogy nem elég, ha megtalálhatóak az adatkezelők vagy adatfeldolgozók adatai (pl. honlapja, e-mail címe, stb.), hanem hogy valóban szolgáltatásokat kíván az éritettnek nyújtani. Ezt úgy lehet ellenőrizni, hogy az adatkezelő olyan nyelvet vagy pénznemet választott, ami lehetővé teszi az érintett számára az áruk vagy szolgáltatások igénybe vételét.

Akkor is alkalmazni kell a rendeletet, ha a tevékenységet végzők az érintettek viselkedését kívánják monitorozni. Az interneten való megfigyelés egyik legfőbb célja, hogy az érintettet teljesen kiismerjék, megtudják mik az általa kedvelt dolgok, mik iránt érdeklődik és milyen szokások fedezhetők fel az internet használata közben. A mesterséges intelligenciák megalkotása során a mind ezek által megszerzett információt használják fel, hogy a személyre szabott ajánlásokat, reklámokat tudjanak küldeni.

A területi hatály esetén két dolgot kell figyelembe venni. Azt, hogy az adatkezelés alanyának hol van a tartózkodási helye, illetve hogy mi az adatkezelő és az adatfeldolgozó tevékenységi helye. Ezért tehát, nem számít, hogy hol állampolgár az alany, valójában hol mennek végbe az adatkezelő munkálatok és az sem hogy az adatkezelőnek vagy adatfeldolgozónak hol van az központja. Mind ezek miatt már nem alkalmazható a forum shopping elve, mivel elkerülhetetlen a GDPR alkalmazása. A rendelet vonatkozik arra az esetre is, amikor egy társaság tevékenységi helye az Unióban található és a nem az EU-ban tartózkodó érintettek személyes adatait kezelik. (JÓRI-SOÓS-BÁRTFAI-HÁRI, 2018) Azonban, ha valaki egy EU-n kívüli országban tartózkodik Uniós állampolgárként, és olyan vállalat kezeli az adatait addig amíg ott van, ami nem tartozik az Európai Unió tagállamai közé és nem is végzi ott tevékenységét, akkor ebben az esetben nem kell alkalmazni a GDPR szabályait. A következő ábra könnyítheti a területi hatály megértését:

Érintett állampolgársága	Érintett tartózkodási helye	Adatkezelő/adatfeldolgozó tevékenységi helye*	GDPR hatálya alá tartozik?	
			Igen / Nem	Ha igen, akkor melyik pont alapján
EU	EU	EU	✓	3. cikk / 1. pont
EU	EU	Nem EU	✓	3. cikk / 2. pont**
EU	Nem EU	EU	✓	3. cikk / 1. pont
EU	Nem EU	Nem EU	×	
Nem EU	EU	EU	✓	3. cikk / 1. pont
Nem EU	EU	Nem EU	✓	3. cikk / 2. pont**
Nem EU	Nem EU	EU	✓	3. cikk / 1. pont
Nem EU	Nem EU	Nem EU	×	

5.sz. ábra: A rendelet területi hatálya

Ezek alapján tehát világosan látszik, hogy a rendelet nem csak az EGT-államaira vonatkozik, hanem azokra is akik ezekkel az országokkal adattovábbítást végeznek.

Különleges helyzetbe került az Egyesült Királyság az Európai Unióból való kiválása után. Mivel korábban ő is tagja volt az EGT-nek és ezáltal azok az országok közé tartozott akiknek meg kellett újítaniuk az adatvédelmi jogrendszerüket, így ők is szabadon továbbíthattak adatokat a többi tagállamba.

A Brexit 2020. január 31-i bekövetkezése után azonban ez megváltozott. Kérdésessé vált, hogy vajon a kiválás után is megfelelnek e az országban alkalmazásban álló szabályok, a GDPR szigorú biztonsági feltételeinek. Az Egyesült Királyságnak két opciója volt az Európai Unióból való kiválása után, vagy megfelelőségi határozatot szerez, vagy ha maguk az adatkezelők vesznek igénybe valamilyen szerződéses formát az egymás között végbemenő adattovábbításokhoz.

A kilépés során elfogadott megállapodás azonban az Egyesült Királyság 2020. december 31-ig egy úgynevezett átmeneti időszak tartott. Ebben az időszakban továbbra is az Uniós előírások vonatkoztak az Egyesült Királyságra, így az adattovábbítás szempontjából sem változott semmi az év végéig. Ez idő alatt a megfelelőségi határozat megszerzése volt célja az országnak, de ez nem történt meg.

Azonban az kérdések vetett fel a szigetországgal kapcsolatban álló vállalatokban, hogy az átmeneti időszak elteltével milyen szabályok vonatkoznak majd rájuk és milyen feltételeknek kell eleget tenniük, tevékenységük továbbra is zökkenőmentes működése érdekében. Erre 2020. december 24-ig kellett várniuk, hiszen ezen a napon született meg egy megállapodás, ami rendezi ezt a kérdést. Ekkor fogadták el a UK GDPR névre hallgató szabályzatot, ami szinte teljesen megegyezik a GDPR-ral. Ennek 2021. január 1-i életbe lépése után 4 hónapig még minden marad úgy, ahogy kiválása előtt volt, tehát továbbra is szabad az adatok továbbítása. Ezt a 4 hónapot, ha mindkét fél (az EU és az Egyesült Királyság) beleegyezik, akkor 2 hónappal ki lehet még bővíteni. Így tehát az Egyesült Királyság célja az, hogy 2021. július 1-ig megkapja a rájuk vonatkozó megfelelőségi határozatot.

Ennek érdekében viszont változtatások eszközölésére lesz szüksége a szigetországnak. Az Egyesült Királyságnál is az a helyzet áll fenn, mint az USA-ban. A Schrems II. ügy kapcsán hatályon kívül helyezett EU-UK Privacy Shield is hasonló okok miatt került megszüntetésre. Az adatvédelmi pajzsnak azért kellett megsemmisülnie, mert

bebizonyosodott, hogy az amerikai nemzetbiztonsági szervek korlátlanul megszerezhetik az emberek adatait, amik így nincsenek megfelelő mértékben védelem alatt. Ez a gond a brit titkosszolgálatoknál is észlelhető. 2020 őszén az Európai Bíróság megállapította, hogy az ország titkosszolgálatai korlátlan mennyiségű adathoz juthatnak hozzá az internetes és telefonos szolgáltatókon keresztül, ami az általános adatvédelmi rendeletben szereplő szabályozások alapján nem megengedett. Kérdéses, hogy az Európai Bizottság miként fog dönteni, annak fényében, hogy a Privacy Shield is éppen ilyen okok miatt került megszüntetésre. Amennyiben elutasítják az Egyesült Királyság megfelelőségi határozat iránti kérvényét, sokkal nehezebb helyzetbe sodor minden olyan országot, amelyek szeretnének felkerülni a határozattal rendelkezők listájára, hiszen nagyon magas elvárások elő állítanák őket. Azonban arra is számítani lehet, ha meg is kapja a szigetország a határozatot, akkor is lesznek olyanok, akik az Európai Bíróság elé vinnék az ügyet.

Mindenki számára előnyösebb lenne, ha a Bizottság a határozat elfogadása mellett döntene, mivel az Egyesült Királyságnak nagy szerepe van a globális adatforgalomban. Ők bonyolítják le ennek körülbelül 11százalékát. Nagy veszteség lenne nem csak a szigetország, hanem mindenki számára, ha ez az Európai Unióból való kiválásuk miatt romlana.

5.3 Adattovábbítás harmadik országba

A fejezet eddigi részében ismertettem, hogy melyek a tagok és társult tagok a GDPR tekintetében, illetve hogy milyen helyzetekben kell alkalmazni a rendeletet. Már láthattuk, hogy ez nem csak az EGT-államaira van hatással, hanem a harmadik országbeli adatkezelőkre és adatfeldolgozókra is vonatkozik a szabályozás, extraterritoriális hatással.

Nehezebb helyzetbe kerültek azok a vállalkozások, amelyeknek tevékenységi központjuk egy harmadik országban van és rendszeresen hajtanak végre személyes adatok továbbítást, mivel ebben az esetben rájuk is vonatkozik a GDPR, mert már az Uniós érintett személye számít nem pedig az adatkezelés helye. Tehát, ha egy harmadik országba, vagy nemzetközi szervezet számára továbbítanak bizonyos személyes adatokat, majd adatkezelési folyamatok mennek végbe rajtuk, csak abban az esetben van lehetőség, ha az adatkezelő és az adatfeldolgozó eleget tesz a rendeletben szereplő szabályoknak és biztosítja az adatok védelmét. Így azzal a hibás közvélekedéssel szemben tehát, hogy nem

szabad EGT-n kívüli országba adatot továbbítani, úgy igaz a megállapítás, hogy csak abban az esetben nem mehet végbe a folyamat, ha az adott ország nem képes eleget tenni a rendeletben meghatározott biztonsági szintnek.

Ezekből látszik, hogy szigorú feltételek mellett kerülhet csak sor harmadik országbeli adattovábbításra, hiszen az alapelvek betartása mellett a rendelet V. fejezetében található feltételek legalább egyikének teljesülnie kell. Három nagyobb csoportba oszthatók a feltételek:

1. megfelelőségi határozat alapján történő adattovábbítás
2. megfelelő garanciák mellett történő adattovábbítás
3. különös helyzetekben a GDPR biztosít eltérési lehetőséget.

Az egyik lehetősége az adattovábbításnak a megfelelőségi határozat megszerzése, amit az Európai Bizottság bírál el. Ehhez szükséges, hogy a határozatot igénylő ország megfeleljen a rendeletben szereplő alapjogoknak és olyan szintű legyen a védelem, mint az Uniós jogban, azonban az ehhez felhasznált eszközök nem kell, hogy teljes mértékben megegyezzenek az EU-ban használtakétól. Az Európai Bizottság feladata, hogy megvizsgálja az adott ország adatvédelmi szintjét és amennyiben azt megfelelőnek tartja, megfelelőségi határozatot adhat ki. Ha egy ország megszerzi ezt a határozatot, akkor további teendők nélkül mehet végbe a személyes adatok továbbítása.

Azonban az EUB (Európai Unió Bírósága) döntése alapján, a felügyeleti hatóságoknak vannak hatásköreik akkor is, ha korábban az Európai Bizottság megfelelőségi határozatot adott egy országnak, de egy érintett személyes adatainak kezelése során arra hivatkozott, hogy az országban nem megfelelő mértékben vannak védve az adatai. A kiadott megfelelőségi határozatok állandó megfigyelés alatt állnak az Európai Bizottság által. Fontos szerepe van ennek, hiszen ha úgy vélik, hogy többé már nem felelnek meg a határozatban leírtaknak, akkor módosíthatják, felfüggeszthetik vagy hatályon kívül helyezhetik azt.

Jelenleg Andorra, Argentína, Kanada (csak bizonyos szervezetek), Feröer-szigetek, Guernsey-sziget, Jersey-sziget, Izrael, Japán, Man-sziget, Új-Zéland, Svájc és Uruguay bizonyult méltónak a határozat megszerzésére.)

Amerikában speciális helyzet állt elő, mivel nem kaphatták meg a megfelelőségi határozatot, de 2016. július 12-én elfogadott az Európai Bizottság egy EU-USA adatvédelmi pajzs (EU-US Privacy Shiled) nevű keretrendszert. Azok a vállalatok, amelyek önként tanúsítják, hogy megfelelnek az adatvédelmi pajzsban szabályainak, azok felkerülhet a listára, aminek a célja a kereskedelmi célból továbbított adatok

védelme. Azok a szervezetek, amelyek felkerültek a listára, ugyan úgy, mint egy megfelelőségi határozat megszerzése esetén , minden további kötelezettség nélkül végezhetnek adattovábbítást. Évente ellenőrzik együtt, hogy a rendszer továbbra is megfelel e az elvárt előírásoknak. Jelenleg több mint 5000 vállalat szerepel a listán.

Abban az esetben, ha egy országnak nincs megfelelőségi határozata vagy egy amerikai cég nem szerepel az adatvédelmi pajzs listáján, akkor az adatkezelőknek és adatfeldolgozóknak megfelelő garanciákat kell vállalniuk. Lehetőségük van olyan garanciákat vállalni, amikhez nem kell az illetékes felügyeleti hatóság külön engedélye, viszont olyan is, amihez szükséges az ő engedélyük. Az engedélyt nem igénylő garanciák a kötelező erejű vállalati szabályok (Binding Corporate Rules, BCR) használata, magatartási kódexek, tanúsítási mechanizmus vagy a Bizottság által elfogadott általános adatvédelmi kikötések. (EURÓPAI ADATVÉDELMI JOGI KÉZIKÖNYV, 2018)

A Bizottság által elfogadott általános adatvédelmi kikötéseknek, vagyis az úgynevezett modellszerződéseknek jelenleg két fajtája van, két adatkezelő között, illetve adatkezelő és adatfelhasználó között végbemenő adattovábbítás biztosítására. Két adatkezelő között történő adattovábbításra vonatkozó modellszerződést találhatunk két különböző határozatban is, viszont adatkezelő és adatfeldolgozó között történő folyamat bekövetkezése esetén csak egy határozatot kell figyelembe venni ahhoz, hogy biztosítva legyenek a megfelelő garanciák. Tehát a modellszerződések valamelyikének megkötésével, teljesülhetnek a garanciák, ami által szintén szabadon áramolhatnak az adatok a szerződést megkötttető felek között.

A magatartási kódex is lehetőséget kínálhat arra, hogy az adattovábbítás szabadon megtörténhessen. A magatartási kódexben az adatkezelők és adatfeldolgozók bizonyos tulajdonságait (pl. tisztességes és átlátható adatkezelés, adatok gyűjtése, érintettek jogainak figyelembe vétele, stb.) vizsgálják meg annak érdekében, hogy megállapítható legyen, az adott esetben megfelelnek az adatvédelmi szabályoknak és helyesen járnak e el bizonyos helyzetekben. Ha ezek a feltételek teljesülnek, jogosulttá válnak az adattovábbításra.

A jóváhagyott kötelező erejű vállalati szabályok (BCR) használatára abban esetben kerülhet sor, amennyiben ugyan olyan tevékenységet végző vállalatok vagy megegyező vállalatcsoportok között jön létre az adattovábbítás. Ezt azonban csak akkor lehet megfelelő garanciának tekinteni, ha a felügyeleti hatóság előzetesen elfogadta, amihez az szükséges, hogy a vállalati szabályok kitérjenek bizonyos adatvédelmi elvekre

is. Amennyiben elfogadásra kerültek a szabályok a fő felügyeleti hatóság által, amit megelőz az Európai Adatvédelmi Testület véleménye, akkor a vállalatok között szabadon létrejöhet az adatok továbbítása.

Amennyiben egy ország esetében sem megfelelőségi határozat, sem megfelelő garanciák nem teljesülnek, abban az esetben jöhet szóba a GDPR különös helyzetekben eltérő lehetőségei. Ilyen lehetőségek lehetnek például, ha az érintett hozzájárulását adja, annak ellenére is, hogy tájékoztatták az esetleges veszélyekről a megfelelőségi határozat és a garanciák meglétének hiányából fakadóan, vagy ha az érintett és az adatkezelő között megkötttendő szerződés elvégzéséhez vagy annak előkészületeihez szükséges az adattovábbítás, ha valamilyen közérdekből lényeges, ha az érintett érdekeit védi, de az valamilyen oknál fogva nem tudja engedélyét megadni, ha szerződés létrehozása a cél az adatkezelő és egy harmadik személy között az érintett védelméért. (EURÓPAI ADATVÉDELMI JOGI KÉZIKÖNYV, 2018) Tehát ha ezek közül a feltételek közül legalább egy bizonyíthatóan fennáll, akkor az engedély megszerzése után az adattovábbítás létrejöhet.

Azonban a szerződéses kikötésekkel kapcsolatban felmerült egy probléma, ami megkérdőjelezett pár dolgot, ezt az ügyet Schrems-ügynek nevezik. A szóban forgó problémát Max Schrems vetette fel miután az EUB visszavonta a biztonságos kikötő névre hallgató határozatot. Ennek a határozat a lényege az volt, hogy az Európai Unió és az Amerikai Egyesült Államok között létrejöhessen adattovábbítás, úgy hogy a szabályozásokat a korábban már megismert 95/46/EK irányelvhez igazítják, annak kielégítése érdekében. Mivel ez a határozat már nem volt érvényben, így más módját kellett keresni az adattovábbításnak és több amerikai vállalatnak is az általános szerződéses feltételekre esett a választása, ezek között a cégek között szerepelt a Facebook Ireland is. Schrems ekkor az ír hatóságokhoz fordult azzal a kérésével, hogy hagyják abba az adatok USA-ba való továbbítását, mivel ezeknek a folyamatoknak a lefolyása során nincsen biztosítva az adatok védelme.

Később az ügy az EUB elé került Schrems II. néven. Ott az a döntés született, hogy a korábban már bemutatott EU-US Privacy Shield érvénytelenné válik, így az USA-ba történő adattovábbítás már csak szerződéses alapon történhet meg.

Abban az esetben ha sem megfelelőségi határozattal nem rendelkezik egy ország, illetve nincsenek meg a megfelelő garanciák és nem teljesül az előbb felsorolt esetek

közül egyik sem, akkor is van még lehetőség az adattovábbításra. Csak akkor lehetséges ez, ha egyszeri adattovábbításról van szó, csak limitált számú érintettre vonatkozik, az adatkezelő valamilyen kényszerítő erejű jogos indokkal, amihez képest az érintett érdekei csak másodlagosak és ha az adatkezelő az adattovábbítás helyzetét kielemezte és az adatok védelmére biztosítani tudja. Ha ezek a feltételek teljesülnek, akkor az adatkezelőnek kötelessége értesíteni az érintettet és informálnia arról is, hogy milyen kényszerítő erő miatt van szükség az adattovábbításra.

Különleges esetekben nemzetközi megállapodások keretein belül is lehetséges az adattovábbítás harmadik országokkal vagy nemzetközi szervezetekkel, abban az esetben, ha ezek megfelelő garanciákat vállalnak a személyek adatainak védelme érdekében. Ezekre a megállapodásokra nem terjed ki az adatvédelmi rendelet. Ilyenek például az utasnyilvántartások (PNR). Megállapodást kötött az EU Ausztráliával, Kanadával és az USA-val, annak érdekében, hogy megelőzhessék a bűncselekményeket, illetve azok felderítése könnyebb legyen. Ezeket az adatokat a jegyvásárlás folyamata közben gyűjtik össze az utasokról, amiket aztán a légitársaságok kereskedelmi célokra is felhasználnak. 2016-ban hagyta jóvá az Európai Unió az EU-PNR néven ismert irányelvet. Ez a szabályzat tartalmazza a harmadik országbeli hatóságok számára küldött adatok megfelelő módját is, szintén annak érdekében, hogy megelőzhetők legyenek a bűncselekmények, illetve a nyomozás könnyebben végbe mehessen. Ebben az esetben, külön elbírálásra van szükség, hogy valóban elkerülhetetlen az adatok továbbítása és jogosan kérik azokat.

Amikor először, 2014-ben írt alá az EU egy ilyen megállapodást, ellenőrizni kellett, hogy az abban leírtak nem sértik e meg az Alapjogi Chartában szereplő alapjogokat. Ekkor ezt az ügyet az Európai Unió Bírósága elé vitték, ahol az a döntés született, hogy a megállapodás a jelenlegi formájában nem felel meg és nem összeegyeztethető az Alapjogi Chartával. Azzal indokolták döntésüket, hogy az adatok összegyűjtése sérti a magánélethez való jogot, mivel az adatok által elemezhető lett volna az érintettek szokásai, egészségügyi állapota, vagyoni helyzete. Mind ezek alapján arra jutott az EUB, hogy a megállapodásban leírtak nem felelnek meg a feltétlenül szükséges kikötésnek. (EURÓPAI ADATVÉDELMI JOGI KÉZIKÖNYV, 2018)

Egy másik példa a nemzetközi megállapodásokra a SWIFT (Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság) és az USA Pénzügyminisztériuma között merült fel a terrorizmussal kapcsolatos nyomozások segítéséért. A SWIFT

központja Belgiumban található és ezen a társaságon megy keresztül minden európai bankból útnak indított utalás.

EU véleménye szerint nem volt kielégítők az indokok arra, hogy ezeknek a személyeknek az adatait kiadják a minisztérium számára. Később mégis létrejött egy megállapodás köztük, amiben megfelelő adatvédelmi szabályokat hoztak létre annak érdekében, hogy a terrorizmust meggátolhassák vagy az eljárás elindítását megkönnyítsék, azonban csak kivételes esetekben kerülhetett adattovábbításra sor és ha a lehető legalaposabban határozzák meg, hogy milyen és kiknek az adataira van szükségük.

Minden ilyen kérvény benyújtása során az Europol ellenőrzi annak szükségességét, illetve a megállapodásban szereplő felétételek teljesülését. A kapott adatokat a minisztériumnak maximum 5 évig szabad tárolnia, utána meg kell őket semmisíteniük.

Ez a megállapodás alapból 5 évig volt érvényes, ami 2015-ben telt le és onnantól kezdve évente felülvizsgálják, hogy továbbra is megállja e a helyét.

6. A GDPR JÖVŐJE

Szakdolgozatom eddigi részei által betekintést nyerhettünk az általános adatvédelmi rendelet megalkotása előtti időkbe. Próbáltam bemutatni azt is, hogy mik lehettek az okai a GDPR megalkotásának. Áttekintettem továbbá azt is, hogy napjainkban hogyan operál ez a jogrendszer, milyen akadályokba ütköznek az adatkezelők és adatfeldolgozók tevékenységeik végzése közben, és hogy ezáltal milyen adatvédelmi incidensek jöhetnek létre. A harmadik országokra vonatkozó kikötéseket is ismertettem, amik teljesítésének eredményeképpen az adott országok vagy vállalatok részt vehetnek adattovábbításban. Így tehát összefogó képet kaphattunk a rendelet megalkotásának előnyeiről.

Most azonban arról lesz szó, hogy miben lehetne még fejlődni, annak érdekében, hogy a rendelet még biztonságosabbá tegye az adatkezeléseket, és ezzel ne gátoljon meg más fontos területen való fejlődést.

A jövőre nézve már az európai jogalkotók komoly lépéseket tettek annak érdekében, hogy létrehozzanak egy olyan szabályrendszert is, ami az interneten történő adatkezelő folyamatokat biztonságosabbá teszi. Ezen a területen még sokat lehetne fejlődni. A szóban forgó rendeletnek ePrivacy a neve, amit a GDPR kis testvéreként is

emlegetnek. Ennek a rendeletnek a végső verzióját az Európa Tanács már elfogadta. Az Európa Parlamenttől kapott arra utasítást, hogy indítson tanácskozásokat a rendelet végleges verziójának megalkotásához. Az ePrivacy az elektronikus után történő hírközlés területének korlátozására lett létrehozva.

A rendelet szabályai között szerepel az elektronikus hírközlés által létrejövő metaadatok és ezek tartalmát meg kell védeni. Ilyen típusú hírközlés csak akkor mehet végbe, ha abba beleegyezik mind a küldő, mind a többi érintett, illetve ha csak a szolgáltatás nyújtása a cél. Metaadatnak tekinthető például az elektronikus hírközlésben részt vevők helyrajzi adataik vagy a kapcsolat létrejöttének időpontja. Ezeknek az adatoknak a kezelése csak hálózatkezelés, hálózat-optimalizálás, szerződéses kötelezettségek teljesítése, számlázás, kifizetés-számítás, csalás ellenőrzés, visszaélésszerű használat megakadályozása, illetve tudományos vagy történelmi kutatás céljából mehet végbe. Az Európai Tanács egy tájékoztatójában volt olvasható, hogy a metaadatok beleegyezés általi használata a közlekedés megjelenítése érdekében történhet meg, ami segítheti a állami hatóságokat és a közlekedési szolgáltatókat abban, hogy biztosan jó helyen kerüljön sor a fejlesztésekre. Ezeknek az adatoknak a kezelése az érintett létfontosságú érdekében is megtörténhet. Ilyen eset például, a még jelenleg is zajló koronavírus járvány, mivel az emberek adatai nagy mértékben segítheti a járvány megfigyelését, illetve bármilyen természeti csapásnál ez áll fenn.

A rendelet kitér az érintettek végeszközeivel kapcsolatos adatvédelemre is. Ebben a tekintetben is korlátozásokat fogalmaz meg. Végeszközöknek tekinthetők az érintettek telefonjai, tableteik, illetve minden szoftver- és hardvereszköz. Ezek az eszközök rengeteg olyan információt tartalmaznak, amiket csak az érintett hozzájárulásával lehet kezelni. Ilyenek például a telefonszámok, fényképek, helyrajzi adatok és még sok más is. Ha a felhasználó nem adja hozzájárulását az ezen adatok felhasználására, abban az esetben, csak akkor kerülhet sor ezek kezelésére, ha annak okát a rendelet leírásában megtaláljuk. Ilyen jogos indokok lehetnek az elektronikus hírközlési szolgáltatások nyújtása, a hallgatottság mérése, szolgáltatás- és eszközbiztonsági intézkedések, csalás-megelőzés, különleges körülmények megléte esetén biztonsági célú szoftverfrissítések eszközölése vagy visszahívások esetén az eszköz helyének meghatározása.

Az ePrivacy Rendelet többek között rendelkezik még a tárgyak internete (Internet of Things, IoT) felett is. Az IoT esetében egy olyan hálózatról beszélünk, amelyen belül a használati eszközök össze vannak kapcsolva. Ilyen hálózatnak tekinthetők az okosotthonok, okosautók, gyógyászati segédeszközök, termosztátok, okosmérőeszközök

és még rengeteg ehhez hasonló IoT által működtetett hálózat fel lehetne sorolni. Napjainkban egyre népszerűbbek ezek a rendszerek, mivel nagy mértékben megkönnyíti az életet, mert mindent irányítani lehet egy eszközön keresztül.

Az ilyen eszközök és rendszerek által kezelt adatok és ezek tárolási kapacitásának használata, illetve az ezeken megtalálható információk kezeléséhez nincsen szükség az érintettek beleegyezésére, de csak abban az esetben ha felhasználó által igénybe vett szolgáltatás nyújtásához ez nélkülözhetetlen. Ennek értelmében tehát, ha okosmérőeszközökről beszélünk, akkor szükség van a felhasználó adataira annak érdekében, hogy a szolgáltató pontos képet kapjon az energiahálózat stabilitásáról, hogy biztonságos maradhasson az, illetve az érintett energiafogyasztásának megfigyelése is szükséges a számlák kiállítása miatt. Az okosautóknál is ugyan ez a helyzet áll fenn, hiszen nagyon fontos, hogy a szoftverfrissítések által biztonságosak maradhassanak ezek a járművek, amik az általuk tárult, majd később felhasznált adatok alapján kerül fejlesztésre.

A cookie-k használatát is szabályozni fogja az ePrivacy a bevezetését követően. A cookie (magyarul HTTP-sütinek is szokták nevezni) egy olyan szoftvernek tekinthető, ami információkat gyűjt az érintettekről, majd azokat fel is használja. A rendelet ezen része vonatkozik minden cookie-ra, illetve az ahhoz hasonló rendszerekre is. Az ilyen jellegű szoftverek alkalmazásának során kötelező az érintett hozzájárulását kérni az adatai tárolásához és felhasználásához. Lehetőséget kell adni a felhasználók számára, hogy a sütik nélkül vagy azokkal kívánja igénybe venni a szolgáltatásokat.

A cookie-k használatát úgy kell a szolgáltatóknak beállítani, hogy az érintettek dönthessék el, hogy milyen szintű hozzáférést engedélyeznek az adataik szempontjából, illetve az internetes keresőoldalaknál lehetőségük kell legyen bizonyos szolgáltatók számára is külön meghatározni a hozzáférhetőségüket. Ezáltal szeretné a rendelet arra bíztatni a szolgáltatókat, hogy olyan rendszert alakítsanak ki, amely által a felhasználók könnyedén kezelhetik a cookie beállításaikat, azok átláthatók legyenek, illetve hogy adott esetben ezeket módosítani, vagy akár törölni is tudják, bármikor amikor csak szeretnék. Az érintett belegyezése mindig fontosabb szerepet kell hogy kapjon az önrendelkezés teljesülése érdekében, mint a szoftverbeállítások.

A session cookie-k, aminek lényege, hogy csak az adott munkamenet időtartama alatt tárolja az adatokat, amint bezárásra kerül a böngésző az adatok törlésre kerülnek, nem szükséges az érintett hozzájárulása. Ilyen cookie még a hitelesítő süti is. Ez olyankor kerül használatra, mikor például az internetes vásárlás során a rendszer automatikusan

kitölti a mezőket a kezdőbetűk beírása után. Ezek a cookie-k a kivételek, amikhez nem szükséges a felhasználó beleegyezése.

Végezetül a nem kívánt reklámokat is korlátozni fogja az új rendelet. A rendeletben szereplő szabályozás értelmében nem lehet a szolgáltatók által összegyűjtött adatokat felhasználni célzott reklámok küldése érdekében, csak abban az esetben, ha ebbe az érintett is beleegyezett. Ez mindenféle felületen és formában küldött reklámra vonatkozik, ezáltal beleértve az e-maileket, SMS-eket és a weboldalakon történő reklámozásokat is.

Viszont ha az érintett valamilyen vételezést hajtott végre a szolgáltatónál, akkor attól a szolgáltatótól már kaphat reklám célú üzeneteket, ajánlásokat, a tranzakció során összegyűjtött és felhasznált adatok által. Az érintetteknek azonban jogukban áll ezt a fajta adatfelhasználást megtiltani a szolgáltató számára.

Amennyiben elfogadásra kerül majd ez a rendelet, akkor a GDPR-nál is már tapasztalt két éves türelmi idő után lép majd életbe ez a szabályozás.

Napjainkban a mesterséges intelligencia (Artificial Intelligence, AI) nagy szerepet játszik az életünkben. Rengeteg hasznos innovációt köszönhetünk neki, amik megkönnyítik a mindennapi életünket. Továbbra is nagy technológiai fejlődések várhatóak ezen a területen, hiszen nagyon népszerűvé váltak az ilyen rendszerek.

Azonban a mesterséges intelligencia komoly kérdéseket és problémákat vet fel az adatvédelem területén. A GDPR 2018-as életbe lépése óta igencsak le lettek korlátozva Európában a mesterséges intelligencia lehetőségei. Mivel a rendelet az adatok kezelését és továbbítását nagy mértékben korlátozza az EU körében, így nagy lemaradásba kerülhetnek Észak-Amerikával és Ázsiával szemben, mivel az AI fejlesztésének nélkülözhetetlen rész a nagy adathalmazok. A rendelet óta azonban az adatok gyűjtése nem történhet meg, csak ha arra az adatkezelőnek valami jogos indoka van. (EURÓPAI ADATVÉDELMI JOGI KÉZIKÖNYV, 2018)

A GDPR alapelvei is nagy kihívások elé állította az adatkezelőket a fejlesztési folyamatok során. Mivel a nagy adathalmazokkal történő tevékenység a szerves része a fejlesztésnek, így ez sértheti az adattakarékosság alapelvét. A legtöbb esetben hatalmas mennyiségű összegyűjtött adatra van szükség, amelyek felhasználási célja sincs mindig pontosan meghatározva.

Az előbb leírtak miatt a célhoz kötöttség elvének megvalósulása sem lehetséges, hiszen ennek értelmében csak arra lehet felhasználni az adatokat, amilyen céllal azt összegyűjtötték, vagy ha az érintettek beleegyeznek ennek eltérésétől.

Továbbá a nagy adathalmazok használata sérti a pontosság elvét is, mivel az adatok nagy mennyisége miatt nincs lehetőség azok ellenőrzésére. Nem tudják még azt sem, hogy kit kell felelőssé tenni, ha egy mesterséges intelligenciával működő robot kárt tesz valakiben, illetve annak eldöntése is majdhogynem lehetetlen, hogy egy esetleges incidens esetén a károk szándékosan vagy véletlen következtek be.

Számos más problémát felvet az érintettek jogai körében is a nagy adathalmazok kezelése. Azonban amellett sem szabad elmenni, hogy óriási előnyei vannak ennek, mind például a közösségi hálózat építésében és a szolgáltatók számára is. A jövőben viszont nagy hangsúlyt kell fektetni az előzőekben felsorolt problémák megoldására, hogy az érintettek személyes adatai is kellő mértékben védve legyenek, de közben a mesterséges intelligencia fejlődését sem gátolja meg a rendelet.

Ezeknek az orvoslására az Európai Bizottság nem olyan régen tett egy javaslatcsomagot. Ennek részeként megtiltanák a befolyásolásra kifejlesztett mesterséges intelligenciákat, mert azok nagy hatással lehetnek az érintettek életére. Betiltanák ezen kívül a bankok által használt MI rendszereket is, amelyeket a hitelkérelmek elbírálásánál használnak. Az is fontos szempont lenne, hogy a szolgáltatók részletes tájékoztatást adjanak az érintetteknek, illetve ők bármikor nyomon tudják követni az adatkezelés folyamatát, és ha szükségesnek látják élhessenek a GDPR-ban foglalt jogaikkal.

A világban még nem született meg a megfelelő szabályozás a mesterséges intelligenciára nézve, mivel ez még egy újdonságnak számít. Nehéz feladat és nagy kihívások elé állítja a jogalkotók egy mindent lefedő jogrendszer kidolgozása, ami sem az érintettek sem az adatkezelők számára nem jelent hátrányt. Sok javaslat és panasz is érkezik mindkét oldalról ebben a témában, azonban a megfelelő jogrendszer kialakítása, amely kezeli és megoldja az ezzel kapcsolatban felmerülő problémákat, valószínűleg még sok-sok év munkáját veszi majd igénybe.

Láthatjuk tehát, hogy a GDPR létrejöttének sok pozitív hozadéka is volt, azonban rengeteg kérdés merül fel az alkalmazásával kapcsolatban még mind a mai napig, pedig már idén a hatályba lépésének ötödik évfordulója lesz. Remélhetőleg egyre több ország és vállalat próbál majd megfelelni az álalános adatvédelmi rendelet előírásainak, ami által

megfelelőségi határozatot kapnak, így kiépítve az egész világon biztonságosan, és az érintettek adatainak védelmét szem előtt tartott adattovábbítást.

7. ÖSSZEFOGLALÁS

Az elmúlt években talán az egyik legtöbbet felidézett mozaik szó a GDPR volt. A nem várt nagyságú figyelmet egy új jogszabály kapta meg, amelyet az Európai Unió 2018. május 25-én léptetett életbe általános adatvédelmi rendelet (General Data Protection Regulation, GDPR) néven, aminek a feladat az volt, hogy megújítsa, korszerűsítse és új alapokra helyezze a személyes adatok biztonságát. Amint azt megismerhettük, az adatvédelem története hosszú múlttal rendelkezik, azonban a legtöbb ember ezt csak a rendelet létrejövetele után vette csak észre és ezáltal egyre inkább váltak nyitottabbá, kezdtek érdeklődni az adatvédelem témája iránt. Emiatt dolgozatomban többek között arra próbáltam választ találni, hogy a rendelet létrejötte miként reformálta meg az adatvédelem szabályozását.

Először áttekintettem, hogyan fejlődött az évtizedek során a személyes adatok védelme hazánkban és nemzetközi szinten is, milyen határozatokat hoztak létre. Az adatvédelem a II. világháború után kezdett fontossá válni, hiszen onnantól kezdve a technológia is rohamos fejlődésnek indult, így személyes adatink védelmével kapcsolatban is előre kellett lépni. Eleinte még szinte alig lehetett említéseket találni a személyes adatokról és azok védelméről a különböző szabályozásokban, de az idő elteltével az európai jogalkotókban megfogalmazódott ezek védelmének és biztonságának fontossága. Először 1995-ben közzétett szabályozás alkotta meg a harmonizált, európai szintű adatvédelmet, ami a jelenlegi rendelet létrehozása előtt majdnem két évtizeden keresztül vállalt kezességet Európában a személyes adatok biztonságának megőrzésében, ez az irányelv a 95/46/EK számú volt. Hazánkban a kifejezetten adatvédelemre figyelmet fordító törvényt csak a kilencvenes évek elején, 1992-ben hozta létre az Országgyűlés, amin rengeteg változtatást kellett eszközölni a nem kielégítő alapossága miatt, illetve a társadalmi fejlődés következtében, így 2011-ben a helyébe lépett az Infotörvény. A GDPR és az Infotörvény a mai napig együtt alkotják meg a haza adatvédelmi szabályozás alapjait.

Szakdolgozatom azzal folytattam, hogy hazánk jogrendszerét bemutattam az általános adatvédelmi rendelet hatályba lépése előtt. Majd részletesen ismertettem, hogy milyen szabályozások szerepelnek a GDPR-ban. A rendelet egyik talán leglényegesebb

reformja, hogy annak területi hatálya nem csak az EU tagállamaira és társult tagjaira vonatkozik, hanem ezeken a határokon kívül is érvénybe lép az adattovábbítások esetén. A rendelet azokra is vonatkozik, tevékenységüket nem az Európai Unióban végzik, azonban az általuk kezelt adatok érintettje az EU határain belül található meg.

Az alapfogalmak terén a rendelet két új elvet is megfogalmazott. Ezek az integritás és a bizalmas jelleg elve, illetve az elszámoltathatóság elve alapján az adatkezelőnek tudnia kell bizonyítani a tevékenységének jogszerűségét, ha arra szükség van.

Másik nagyon lényeges része a rendeletnek az érintetti jogok. Részletesen kitértem minden jogra, ismertettem, melyik milyen esetekben vehetők igénybe. Mivel a GDPR középpontjában a személyes adatok és az érintettek védelme, így nagy hangsúlyt fektettek az ő jogaik meghatározása során.

Ezek után az adatkezelők feladatait vettem sorra, amiből kiderült, hogy a rendelet megalkotása és életbe lépése nagy terhet rótt az adatkezelők vállára. Rengeteg előírásnak kellett megfelelniük, és annak érdekében, hogy ez sikerüljön, alaposan ki kell vizsgálniuk a vállalat adatvédelmi szabályozását, ha szükség van rá, kiegészíteni és módosítani kell azt. Ezen kívül sok más lépés megtételére lettek kötelezve a biztonságos adatkezelési folyamat megvalósulása érdekében. Adatvédelmi incidensek is innentől nekik kellett jelenteniük a felügyleti hatóságok felé, hazánkban ez a NAIH.

Szakdolgozatom következő pontjában a GDPR mai helyzetét mutattam be. Ezt a hazai adatvédelmi hatóság adatai alapján tettem meg, amikből tisztán látszott, hogy 2018-ban az emberek még nem voltak teljesen tisztában a GDPR fogalmával és az adatkezelők sem ismerték minden kötelezettségüket. Az idő múlásával azonban ez változott. A vizsgált 3 év alatt majdnem megháromszorozódott a NAIH munkája, mivel egyre több bejelentés és kérelem érkezett feléjük.

Következő fejezetben arra a kérdésre kerestem a választ, hogy mik lehettek a rendelet megalkotásának okai. Egyik eshetőség a forum shopping megakadályozása lehetett, a másik pedig egy olyan Európa kiépítésének lehetősége, amelyben egységesítve és harmonizálva vannak a jogrendszerek annak érdekében, hogy az egyének személyes adatai, ezáltal ők maguk is biztonságban legyenek.

Ez után tértem rá két adatvédelmi incidensre, amelyek megmutatják, hogy mekkora hatalommal ruházhat fel valakit az, ha nagy mennyiségű adathoz jut hozzá. Egyik ügy még a GDPR megalkotása előtt történt Amerikában a 2016-os választások

idején, a másik pedig a tavalyi év legnagyobb bírságát kiszabott ügye volt, amit a világhíres H&M ruházati márka szenvedett el.

Dolgozatom gyakorlatiasabb része következett, mivel itt mutattam be egy weboldal általi példán keresztül, hogy milyen intézkedéseket kellett tenniük az üzemeltetőknek, hogy megfeleljenek a GDPR szigorú és alapos előírásainak. A fejezet végén bemutattam az adatvédelmi hatóságokat, azoknak feladatait, hatásköreit. Ismertettem, hogy a szankcionálás hogyan történik és mi alapján szabják ki a bírságokat.

Jött utána az Európai Unió tagállamaira vonatkozó, azon szabályok bemutatása, melyek teljesítése után szabadon áramolhatnak az adatok a tagállamok között. Rátértem később a harmadik országok, és a külhonos vállalatok esetére is. Arra, hogy miket tehetnek meg annak érdekében, hogy részt vehessenek az adattovábbítási folyamatokban. Külön kitértem az Egyesült Királyság különleges helyzetére, amit a Brexit, vagyis az Unióból való kiválásuk okozott.

Végül pedig próbáltam a GDPR lehetséges jövőjét bemutatni, amiben nagyon sok fejlesztés, módosítás és kiegészítés található majd meg, főleg a mesterséges intelligencia fejlődése érdekében, és hogy a jelenlegi hátráltatott európai helyzetén enyhítsenek. A megalkotás folyamata alatt alló ePrivacy rendeletről is írtam egy keveset, amit csak a GDPR kis testvéreként emlegetnek.

8. IRODALOMJEGYZÉK

CISCO SYSTEMS (2019): https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf , letöltés dátuma: 2021. május 11.

EPRIVACY RENDELET: https://www.naih.hu/files/NAIH_beszamolo_2019.pdf , letöltés ideje: 2021. május 11.

EURÓPAI ADATVÉDELMI JOGI KÉZIKÖNYV (2018): https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf , letöltés dátuma: 2021. május 8.

JAY, R., HAMILTON, A. (1999): Data Protection – Law and Practice. Sweet & Maxwell, London.

JÓRI András, HEGEDŰS Bulcsú, KEREKES Zsuzsanna szerk. (2010): Adatvédelem és információszabadság a gyakorlatban. CompLex Kiadó, Budapest

JÓRI András szerk., SOÓS Andrea Klára, BÁRTFAI Zsolt, HÁRI Anita (2018): A GDPR magyarázata. HVG-ORAC Kiadó, Budapest.

MAJTÉNYI László (2003): Az információs jogok. In: HALMAI Gábor, TÓTH Gábor Attila. Szerk.: Emberi jogok. Osiris Kiadó, Budapest.

MAJTÉNYI László (2006): Az információs szabadságok – adatvédelem és közérdekű adatok nyilvánossága. Complex Kiadó, Budapest.

MAYER-SCHÖNBERGER, V. (1997): General Development of Data Protection in Europe. In: AGRE, P.E., ROTENBERG, M. szerk.: Technology and Privacy: The New Landscape. The MIT Press, Cambridge, Massachussetts.

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (2019): A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről. https://www.naih.hu/files/Beszamolo-2018-MR.PDF , letöltés dátuma: 2021. május 11.

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (2020): A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2019. évi tevékenységéről. https://www.naih.hu/files/NAIH_beszamolo_2019.pdf , letöltés dátuma: 2021. május 11.

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (2021): A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2020. évi tevékenységükről. https://naih.hu/eves-beszamolok?download=349:naih-beszamolo-a-2020-evi-tevekenysegrol , letöltés dátuma: 2021. május 11.

PÉTERFALVI Attila, OSZTOPÁNI Krisztián (2017): A személyes adatok magánjogi védelme a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatában. In:

GÖRÖG Márta, MENYHÁRD Attila, KOLTAY András szerk.: A személyiség és védelme – Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. ELTE Állam- és Jogtudományi Kar, Budapest.

PÉTERFALVI Attila szerk. (2012): Adatvédelem és információszabadság a mindennapokban. HVG-ORAC Kiadó, Budapest.

PÉTERFALVI Attila, RÉVÉSZ Balázs, BUZÁS Péter szerk. (2018): Magyarázat a GDPR-ról. Wolters Kluwer Kft., Budapest

PRIVACY SHIELD LIST: https://www.privacyshield.gov/list , Letöltés dátuma: 2021.május 9.

SZIKLAY Júlia (2011): Az információs jogok kialakulása, fejlődése és társadalmi hatása. Doktori (PhD) értekezés, Pécsi Tudományegyetem, Pécs.

SZŐKE Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése. Infokommunikáció és Jog, 10. évf., 3. szám

SZŐKE Gergely László (2014): Az európai jog megújítása – Tendenciák és lehetőségek az önszabályozás területén. Doktori (PhD) értekezés, Pécsi Tudományegyetem, Pécs.

VOIGT, P. – VON DEM BUSSCHE, A. (2017): The EU General Data Protection Regulation (GDPR). A Particular Guide. Springer

Weltimmo-ügy: https://adatvedelmi.hu/a-weltimmo-ugy-c-23014/ , letöltés ideje: 2021. május 12.

Adequacy decisions – How the EU determines is a non-EU country has an adequate level of data protection. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en , letöltés dátuma: 2021. május 9.

https://www.vg.hu/velemeny/velemeny-rovat-hirei/brexit-uk-gdpr-es-schrems-ii-az-adattovabbitasrol-szol-majd-2021-2-3477073/ , letöltés dátuma: 2021. május 10.

https://gdpr.news.hu/cikkek/itt-az-5-legnagyobb-gdpr-birsag-2020-bol/ , letöltés dátuma: 2021. május 12.

https://www.hwsw.hu/hirek/58575/facebook-scl-cambridge-analytica-pszichografikus-profilozas.html , letöltés dátuma: 2021. május 12.

Jogiszabályok:

1989. évi XXXI. törvény az Alkotmány módosításról

2013. évi V. törvény a Polgári törvénykönyvről

Az Európa Tanács és a Parlament 95/46/EK irányelve (1995. október 24.)

Az Európai Parlament és Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Joganyagok:

Európai Tanács (1950): Emberi Jogok Európai Egyezménye
Európa Tanács (1981): A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezmény (108. számú egyezmény)

Ábrák:

1. sz. ábra: A GDPR előtti szabáylozások
2. sz. ábra: A rendelet létrejövetelének folyamat
3. sz. ábra: A GDPR-ban szereplő jogalapok
4. sz. ábra: Az érintettek jogai
5. sz. ábra: A rendelet területi hatálya