NRTI
Nemzetközi és Regionális Tanulmányok Intézet

Life After the GDPR: Good Data Protection Rules and Prospects for the Future

Élet a GDPR után: jó adatvédelmi szabályok és jövőbeli kilátások

Nemzetközi és Regionális Tanulmányok 16.

Life After the GDPR:
Good Data Protection Rules and
Prospects for the Future

Élet a GDPR után:
jó adatvédelmi szabályok és jövőbeli kilátások

Szeged
2019

A
“Life After the GDPR:
Good Data Protection Rules and Prospects for the Future”

„Élet a GDPR után: jó adatvédelmi szabályok és jövőbeli kilátások”
című konferenciát a Szegedi Tudományegyetem Állam- és Jogtudományi Kar Nemzetközi és Regionális Tanulmányok Intézete és
a Europe Direct Szeged iroda szervezte
2018. október 18-án.

Készült a Szegedi Tudományegyetem Állam- és Jogtudományi Kar
Nemzetközi és Regionális Tanulmányok Intézetében,
az Európai Unió támogatásával.

A kiadvány az Európai Unió támogatásában részesült.
Ez a kiadvány a szerző nézeteit tükrözi, és az Európai Bizottság nem tehető felelőssé az abban foglaltak bárminemű felhasználásáért.

Szerkesztő: Gizem Gültekin-Várkonyi, Sulyok Márton

ISBN 978-963-306-270-8
ISSN 2064-4639

Nyomdai kivitelezés: Innovariant Nyomdaipari Kft.

Tartalomjegyzék
Table of contents

Foreword

Giovanni Buttarelli[1]

Dear Ladies and Gentlemen,

Greetings from Brussels. It is a real pleasure and honor to open your debate today.

First of all, my warm thanks go in particular to the International and Regional Studies Institute of the University of Szeged for the invitation to contribute. I am very sorry for not being with you in person but we are extremely busy finalizing the preparation of the incoming International Conference for Privacy and Data Protection Commissioners. It is a global event this year happening in Brussels only in three days from now, so I am sure you understand.

Speaking about the General Data Protection Regulation, you devoted this conference to discussing the status of adapting national legislation to the new framework, in particular, in Hungary and Poland and the new Regulation has been the reality, we may agree, for almost five months now. Further harmonization and modernization rules were among its key objectives and we should be mindful of a crucial point that the GDPR has not sparked a Copernican revolution. I have said it on several different occasions: what the GDPR has caused is a gentle evolution in the direction of raising the data protection standards worldwide. It is a catalyst for change, it is a game changer.

1 The foreword was transcribed based on the video message of the European Data Protection Supervisor, delivered at the conference.

The GDPR, in fact, seeks to inspire a good form of innovation and inject human values into the market. It aims at reaping the benefits of technology while still enabling citizens to enjoy their (our) fundamental rights to both privacy and data protection. Accountability is a real pillar of the GDPR, which implies acting in full respect of the words and of the spirit of this Regulation which in turn seeks placing a data subject at the very center.

New rights, as the one to data portability, have a great potential for contributing to shaping digital economy in the future. Data Protection by Design and Data Protection by Default will also orient the development of technology and process-design. In this sense, the GDPR sets new parameters for the responsible design and deployment of technology. It requires that companies, designers as well as developers put the interest of the individual at the heart of innovation. The reach of application rules has also evolved with the GDPR; they now apply beyond Europe and this circumstance is crucial in protecting rights in the EU. GDPR has also raised increasing awareness worldwide to the need for better valuing people's rights.

The new Regulation inspires data protection legislation around the world, nowadays one hundred and twenty-eight countries have privacy laws and more are in the making. So it is quite an outstanding result, if you think about how narrow and limited once was the community of countries with legislation in these areas: privacy and data protection. In Europe, we have done our homework, but still, there is a lot to be done.

First, let us consider secondary harmonization. GDPR is a fundamental piece of the framework, but much is left to the margins of maneuver of Member States in some important areas. We have been seeing how approaches vary from country to country. A fair portion of the GDPR's success in this sense will, in my view, depend on how convergent these regulatory choices will be.

Take the age of consent of minors for instance or the more flexible regime for scientific research. Member States may decide to derogate from some rights under specific circumstances. A national legislation

should therefore balance different interests keeping in mind that the right to high standards in terms of data protection is a fundamental right in the EU and therefore convergence should be pursued with this basic aspect in mind.

The second element to consider relates to enforcement. Enforcement of rules is of key importance and it will bring tangible results very soon. Let me say a few words on digital ethics, since I would like to encourage you to widen the angle of the discussion and consider what else should be on the table when dealing with people's fundamental rights.

We have a very ambitious plan to better explore the impact of digital technologies on our lives and the ethical approaches required to orient technology. We will do this with the more than one thousand registered participants, plus guests and people connected in Sofia at our upcoming conference. For an entire week, delegates coming from all over the world, eighty-one countries, will debate Artificial Intelligence, facial recognition and biometrics, attention economy, micro-targeting in political campaigns, tracking and surveillance, digital monopoly, discrimination, and biases, of course, in algorithms. This year's Cambridge Analytica scandal opened Pandora's box. The current revenue model does not seem to be sustainable any longer, it is likely to frustrate people if they are not going to be treated with more dignity and respect. The so-called digital divide, between those who receive benefits from technology and those who are harmed by it, is steadily growing and this is increasingly unfair. So, let me say, there is a huge need to tackle this.

Let me go now onto my concluding remarks, ladies and gentlemen, to say that technologies should be of course developed, deployed anew, but in such a way that they enhance our rights and values and improve our way of life and not the opposite. We are calling then for a renewed sense of responsibility and commitment from all actors involved.

It is now time to wish you a fruitful and engaging day of discussions.

Dr. Trócsányi László[1]

A GDPR jogalkotói nézőpontból

A GDPR születése: intézmények és folyamatok

I. Az uniós adatvédelmi reform három oka

Az EU adatvédelmi reformját, amelynek keretében 2012 és 2016 között megalkották a General Data Protection Regulation-t, azaz a GDPR-t és a kapcsolódó bűnügyi irányelvet, három ok tette szükségessé.

1. A Lisszaboni Szerződés uniós alapjoggá emelte a személyes adatok védelmét

Az adatvédelmi reform egyik okaként – a 2008-as pénzügyi válság kirobbanása idején elfogadott, de csak 2009. december 1-én hatályba lépett – Lisszaboni Szerződést indokolt megemlíteni.

A Lisszaboni Szerződés ugyanis egyrészt uniós alapjoggá tette a személyes adatok védelméhez fűződő jogot (EUMSZ 16. cikk (1) bekezdés), másrészt bevezetett egy új és egységes jogalapot a személyes adatok védelmére vonatkozó szabályok elfogadására (EUMSZ 16. cikk (2) bekezdés).

1 Igazságügyi miniszter, egyetemi tanár, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar

Az EUMSZ 16. cikkének szövege:
(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.
(2) A természetes személyeknek az uniós intézmények, szervek és hivatalok által, illetve az uniós jog alkalmazási körébe tartozó tevékenységeik során a személyes adataiknak a tagállamok által végzett feldolgozása tekintetében történő védelmére, valamint az ilyen adatok szabad áramlására vonatkozó szabályokat rendes jogalkotási eljárás keretében az Európai Parlament és a Tanács állapítja meg. E szabályok tiszteletben tartását független hatóságok ellenőrzik.

Az e cikk alapján elfogadott szabályok nem érintik az Európai Unióról szóló szerződés 39. cikkében említett különleges szabályokat.

Az EUSZ 39. cikkében meghatározott kivétel a közös kül- és biztonságpolitikára vonatkozik, ahol az adatvédelmi szabályokat a Tanács határozatban állapítja meg. Megjegyzést érdemel, hogy a 2012. január 1. óta hatályos magyar Alaptörvény szintén alapjogként ismeri el a személyes adatok védelméhez való jogot annak VI. cikkében.

2. Átmenet az olajalapú gazdaságból az adatalapú gazdaság felé az információs-technológiai forradalom hatására

Az uniós adatvédelmi reform másik okát a korábbi adatvédelmi irányelv (az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról) idejétmúlt szabályozási felfogásában találjuk.

Ezt az irányelvet nem online, hanem offline, azaz papíralapú környezetre alkották, hiszen a ’90-es évek elején-közepén az internet alig-alig volt még ismert Európában. Az elmúlt tizenöt évben zajló információs és technológiai forradalom azonban korábban nem látott ütemű és mélységű gazdasági és társadalmi változásokat idézett (és idéz) elő.

A „nem felejtő" internet, a digitalizáció és ennek eredményeként az automatizáció lehetőségei ugyanis exponenciálisan fejlődnek, és konszenzus van arról, hogy a közeli jövőben minden tartalom szélessávú adatátvitelen keresztül fog eljutni az adatalany-fogyasztóhoz, felváltva a mai olajalapú gazdaságot egy adatalapú gazdasággal.

Az adatalapú gazdaságban exponenciálisan nő a személyes adatok mennyisége, mivel az új technológiákat az ötszáztízmillió uniós polgárból egyre többen és egyre gyakrabban veszik igénybe (pl. okostelefonon keresztül), ezáltal folyamatosan egyre több személyes adatot szolgáltatva magukról az arra nagy érdeklődést tartó adatkezelő-vállalatok számára.

Ahogy az olajalapú gazdaságban a minél több olaj, úgy az adatalapú gazdaságban a minél több személyes adat a profit záloga. Az új technológiáknak köszönhetően ugyanis a szolgáltatást nyújtó vagy terméket árusító vállalatok – személyes adatok birtokában – minden korábbinál nagyobb pontossággal meg tudják találni potenciális ügyfeleiket, és így folyamatosan növelni tudják árbevételüket.

A minél nagyobb árbevétel reményében a vállalatok készek nagy összegeket fizetni a potenciális ügyfelek személyes adataiért. Hogy mekkora a tét, jól szemlélteti az Európai Bizottság azon becslése, ami szerint a félmilliárd uniós polgár személyes adatainak értéke 2020-ra várhatóan el fogja érni az évi ezermilliárd eurót.[2]

Ez a kereslet pedig létrehozott egy olyan új és exponenciálisan fejlődő iparágat, amely óriási mennyiségű személyes adatot gyűjt, rendkívül szofisztikált technológiával elemez, majd nagy haszonnal értékesít e vállalatok számára („*Big Data*"). Ez a technológiai fejlődés új kihívásokat állított a személyes adatok védelme elé.

2 Ld. Viviane Reding biztos 2014. január 27-i beszédét: A data protection compact for Europe. http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm

3. Az adatalany-fogyasztók bizalomhiánya az online szolgáltatásokkal szemben

Az uniós adatvédelmi reform harmadik oka az a komoly fogyasztói bizalomhiány volt, amely a folyamatosan bővülő online szolgáltatásokkal szemben fennállt, és amely végső soron az unió gazdasági fejlődését akadályozta a potenciálisnál kisebb volumenű határon átnyúló online kereskedelem miatt.

Ez a bizalomhiány abból eredt, hogy az 95/46-os adatvédelmi irányelv tág teret adott a tagállamoknak az implementációhoz, így azok jelentős eltéréssel ültethették át az Irányelv szabályait nemzeti jogukba.

Az Irányelv keretszabályai ahhoz vezettek, hogy a tagállamok közül egyesek (pl. Magyarország, Németország, Franciaország) az egyének védelmére helyezve a hangsúlyt szigorú, magas védelmet nyújtó szabályokat alkottak, míg mások (pl. Írország, Luxemburg, Egyesült Királyság) az adatok szabad áramlásának biztosítása céljából a multinacionális vállalat-csoportok érdekeit helyezték előtérbe, és enyhébb, alacsonyabb védelmi szintet biztosító normákat alkottak a nemzeti jogukban. (Az ír adatvédelmi biztos alig két tucat munkatársa között a Schrems-ügy[3] kirobbanásáig nem is volt jogász végzettségű, miközben a Facebook, Amazon, Google, Apple európai központjai kivétel nélkül Írországban vannak.)

3 2013-ban Maximilian Schrems osztrák joghallgató, adatvédelmi aktivista panaszt tett az ír adatvédelmi biztosnál azért, mert személyes adatait a Facebook Ireland az Egyesült Államokba továbbította a Facebook, Inc.-nek. Az ír adatvédelmi biztos a panaszt elutasította arra hivatkozva, hogy az Európai Bizottság 2000-ben hozott határozata szerint az Egyesült Államok és az EU közötti Safe Harbor Agreement az adatvédelem megfelelő szintjét biztosította. A határozat bírói felülvizsgálatát elvégző High Court az EU Bíróságához fordult. Az EU Bírósága 2015-ben kimondta (Európai Bíróság C-362/14 sz. ügy. Maximillian Schrems és a Data Protection Commissioner. A Bíróság 2015. október 6-án kelt ítélete, ECLI:EU:C:2015:650), hogy az európai adatvédelmi hatóságok létező nemzetközi szerződésektől függetlenül bármikor vizsgálhatják az adattovábbítás jogszerűségét, illetve hogy az akkori EU-USA Safe Harbor Agreement nem megfelelő.

Mindez egy olyan töredezett adatvédelmi jogi keretet eredményezett az EU belső piacán, amely az adatalanynak eltérő szintű védelmet nyújtott, és ez (a nyelvi és egyéb okok mellett) nem ösztönözte őket a határon átnyúló online szolgáltatások igénybevételére.

A GDPR előtti, az adatalany-fogyasztó számára előnytelen jogi keretet jól szemlélteti az alábbi példa:

Ha például egy magyar érintett a Facebookkal vagy a Google-lel szemben jogellenes adatkezelés miatt panaszt akart benyújtani, akkor azt kizárólag az ír adatvédelmi biztosnál tehette meg, mivel Írországban van a Facebook székhelye, ráadásul angol nyelven. A panaszt, ha egyáltalán elbírálták, akkor csak az ír jog alapján. Mivel az ír jog nem adott bírságolási jogot (a magyar joggal ellentétben), közigazgatási bírság kiszabására nem volt mód. És az ír biztos határozatát csak ír bíróság előtt lehetett megtámadni. A magyar adatalany legfeljebb azt indítványozhatja az ír bírónál – ír ügyvéd igénybevételével –, hogy forduljon az Európai Unió Bíróságához előzetes döntéshozatali eljárás keretében.

II. Mely intézményben és mikor merült fel elsőként, hogy szükség van a GDPR-ra és a kapcsolódó irányelvre?

Először az Európai Bizottság vetette fel az uniós adatvédelmi jogi keret reformjának gondolatát 2009 júniusában, mégpedig azon közleményében, amely a Stockholmi programot készítette elő. (A Stockholmi Program határozta meg a 2010 és 2014 közötti időszakra az Európai Unió prioritásait azzal a céllal, hogy a polgárok érdekeit és szükségleteit középpontba helyező intézkedésekkel tovább erősítse a jog érvényesülésén, a szabadságon és a biztonságon alapuló térséget.)

A bizottsági közlemény szerint:
„Az Uniónak a személyes adatok védelmére vonatkozó egységes szabályozásra van szüksége, amely az összes uniós hatáskörre kiterjed. A magánéletet tiszteletben tartó technológiák, termékek és szolgáltatások esetében vizsgálni kell európai tanúsítvány létrehozatalának lehetőségét. Az adatvédelem terén intenzív nemzetközi együttműködés szükséges. Az Uniónak hozzá kell járulnia az e tárgyra vonatkozó nemzetközi normák kidolgozásához és fejlesztéséhez."

Az Európai Parlament üdvözölte az Európai Bizottságnak az uniós adatvédelmi reformmal kapcsolatos felvetését 2009 novemberében, és egyebek mellett felszólította a Bizottságot a bűnügyi személyes adatok továbbítását szabályozó kerethatározat felülvizsgálatára.

Egy hónappal később az Európai Tanács (EiT) elfogadta – az Európai Bizottság júniusi közleményén alapuló – Stockholmi Programot. Az EiT ebben a programban felkérte az Európai Bizottságot, hogy értékelje az uniós adatvédelmi eszközök működését, valamint hogy – amennyiben szükséges – terjesszen elő további jogalkotási és nem jogalkotási kezdeményezéseket.

2010 áprilisában a Bizottság közzétette a Stockholmi Program végrehajtására irányuló Cselekvési Tervét, amelynek középpontjában az alapjogok védelmének kihangsúlyozása állt, így többek között a személyes adatok védelmének megerősítése. A Cselekvési Terv hangsúlyozta annak szükségességét, hogy az összes uniós szakpolitika terén gondoskodni kell a személyes adatok védelmére vonatkozó alapvető jog következetes alkalmazásáról.

Egy hónappal ezt követően a Bizottság az Európai Digitális Menetrendben (amelynek célja az egységes digitális belső piac kiépítéséhez szükséges intézkedések felvázolása) központi szerepet szánt a személyes adatok védelmének, ezért 2010-es határidővel „4. kulcsintézkedésként" jelölte meg az adatvédelmi szabályozási keret felülvizsgálatát a felhasználók bizalmának erősítése és jogainak megszilárdítása érdekében.

A 2010-es év végén (novemberben) a Bizottság a „személyes adatok Európai Unión belüli védelmének átfogó megközelítése" című közleményében arra a következtetésre jutott, hogy az Európai Uniónak átfogóbb és következetesebb politikára van szüksége a személyes adatok védelméhez fűződő alapvető jog tekintetében.

III. Széleskörű konzultáció az érintettekkel és az érdekelt szervezetekkel 2009 és 2011 között

Az előbb említettek mellett az Európai Bizottság kétéves, széleskörű konzultációt is folytatott az érdekeltekkel.

2009 május és december között az Európai Bizottság szervezésében került megrendezésre egy magas szintű adatvédelmi konferencia, majd az első nyilvános bizottsági konzultáció.

2010 júniusában sor került célzott konzultációkra a kulcsfontosságú érdekeltekkel, így például külön események valósultak meg a tagállami hatóságok és a magánszektor érdekeltjei, valamint olyan fogyasztóvédelmi szervezetek számára, amelyek a magánélet védelmére és az adatvédelemre specializálódtak.

2010 novemberére az Európai Bizottság akkori alelnöke, Viviane Reding, aki egyben az adatvédelemért felelős biztos is volt, kerekasztal-megbeszélést szervezett az adatvédelem reformjáról. Az ezt követő két hónapban pedig az Európai Bizottság lefolytatta a második nyilvános konzultációját.

2011. január 28-án (az adatvédelem napján) az Európai Bizottság és az Európa Tanács együttes szervezésében magas szintű konferenciát tartottak az uniós jogi keret reformjához kapcsolódó kérdésekről, valamint az egész világra kiterjedő közös adatvédelmi szabályok szükségességéről.

2011 januárja és decembere között pedig az alábbi eseményekre került sor:

- a magyar és lengyel soros tanácsi elnökség során két adatvédelmi konferenciát tartottak (júniusban és szeptemberben);
- az Európai Bizottság műhelytalálkozót szervezett azon tagállami hatóságoknak, ahol megvitatták a büntetőügyekben folytatott rendőri és igazságügyi együttműködés területén felmerülő adatvédelmi problémákat;
- az EU Alapjogi Ügynöksége is konzultációra hívta az érdekelteket „Adatvédelem és a magánélet védelme" címmel;
- júliusban került sor az adatvédelmi reform kulcsfontosságú kérdéseinek megvitatására a nemzeti adatvédelmi hatóságok részvételével;
- az Európai Adatvédelmi Biztos átfogó véleményt adott ki az Európai Bizottság 2010. novemberi közleményében felmerült kérdések vonatkozásában;
- az Európai Parlament július 6-i állásfoglalásával jóváhagyott egy, az adatvédelmi keret átalakítására vonatkozó bizottsági megközelítést támogató jelentést;
- a magyar soros tanácsi elnökség alatt az Európai Unió Tanácsa (BIÜT - Bel- és Igazságügyi Tanács) 2011. február 24-én elfogadott következtetéseiben általában véve támogatta a Bizottság adatvédelmi keret reformjára irányuló törekvéseit és egyetértett az Európai Bizottság megközelítésének számos elemével;
- az Európai Gazdasági és Szociális Bizottság ugyancsak támogatta az uniós adatvédelmi szabályok valamennyi tagállamban való következetesebb alkalmazásának biztosítására vonatkozó bizottsági célkitűzést, valamint a 95/46/EK irányelv megfelelő felülvizsgálatát.

Mindezekből a konzultációkból az derült ki, hogy az érdekeltek nagy többsége szerint továbbra is érvényesek az adatvédelem általános elvei, azonban az 95/46-os irányelvet modernizálni kell az új online

technológiák drámaian gyors fejlődéséből eredő kihívásoknak megfelelően. Kritikával leginkább az uniós személyesadat-védelem széttagoltságát illették, és az abból eredő jogbizonytalanságot, amiért sürgették az uniós szabályok harmonizálását.

2011 második felében, a konzultációk után az Európai Bizottság elkészítette a lehetséges szabályozási alternatívák hatásvizsgálatát. Az alternatívák az alábbiak voltak:

- legkevesebb jogszabály-módosítás,
- meghatározott problémákat egyenként kezelő módosítás,
- átfogó, egységes és részletes jogharmonizáció, valamint azok végrehajtására egy uniós ügynökség létrehozása.

IV. Az uniós adatvédelmi reformcsomag bizottsági benyújtása

2012. január 25-én az Európai Bizottság benyújtotta az adatvédelmi reformcsomagot, amely egy kilencvenegy cikket tartalmazó általános adatvédelmi rendelet-tervezetből, egy bűnügyi hatóságok közötti adattovábbítási irányelv-tervezetből, valamint egy bizottsági közleményből állt. A csomagot egy terjedelmes bizottsági hatásvizsgálati anyag egészítette ki.

Az Európai Bizottság eredeti terve az volt, hogy már 2014 tavaszára, tehát még az európai parlamenti választások előtt, lezárásra kerül mindkét javaslat. Az Európai Parlament kezdettől fogva üdvözölte ezt az ambiciózus tervet.

V. Tárgyalási folyamat a Tanácsban: négyéves intenzív munka

A Tanácsra kezdettől fogva két intézményből, egyrészről az Európai Bizottság, másrészről az Európai Parlament részéről nagy nyomás helyeződött a reformcsomag mielőbbi elfogadása érdekében.

Ennek megfelelően a dán tanácsi soros elnökség alig néhány héttel a GDPR bizottsági benyújtása után, már 2012. február második felében megkezdte a GDPR szakértői szintű tárgyalását, amit további tizennégy egész napos ülés követett.

A tanácsi tárgyalások – a Bizottság és a Parlament nyomására – még intenzívebbé váltak a 2012 júliusa és 2015 decembere közötti soros elnökségek alatt.

A GDPR-ral kapcsolatos intenzív munkát jól szemlélteti nem csak a több mint százhatvan tanácsi munkacsoport-ülés, vagy az, hogy a COREPER, a tagállamok állandó képviselőinek tanácsa, közel negyven alkalommal tárgyalta meg a GDPR-t, hanem leginkább az, hogy három és fél éven át (2012 júliusa és 2015 decembere között) valamenynyi formális és informális bel- és igazságügyi miniszteri tanácsülésen a GDPR volt az első számú vitás napirendi pont.

A tanácsi tárgyalások formálisan végül 2016 elején, a holland soros elnökség alatt zárultak le.

A tanácsi tárgyalások elhúzódásának fő oka abban keresendő, hogy a tagállamok többségének komoly koncepcionális aggálya volt a GDPR bizottsági javaslatával. Ezek a tagállami aggályok ugyanakkor nem a szubszidiaritás és arányosság elveivel voltak összefüggésben, így a nemzeti parlamentek véleménynyilvánítása alapvetően támogató volt, és nem vezetett sárga lapos eljáráshoz.

1. A maximum harmonizációs rendeleti forma

Koncepcionális aggályt, azaz *red line*-t jelentett számos tagállam, köztük Magyarország számára is, a GDPR maximum harmonizációs jellegű rendeleti formája. A Bizottság azzal érvelt, hogy ezzel a (politikai) döntéssel orvosolható a 95/46-os irányelv nagy hiányossága, és érhető el egy egységes uniós adatvédelmi jogi keret, ami jogbiztonság mellett elősegíti a személyes adatok határon átnyúló gördülékeny áramlását is.

A tagállamok viszont rámutattak annak a kockázatára, hogy az uniós adatvédelmi reform következtében számos tagállamban több ponton csökken az adatvédelmi szint, mivel a rendelet hatályba lépése után csak ott és csak annyiban tarthatnak hatályban, vagy alkothatnak a rendelettől szigorúbb védelmet nyújtó nemzeti szabályokat, ahol és amennyiben arra a rendelet kifejezetten felhatalmazást ad (pl. munkajogi terület).

A maximum harmonizációs jellegű rendeleti forma Magyarország számára azért volt *red line*, mert a 2011-ben elfogadott Infotv. megalkotásakor a magyar törvényhozó nemcsak a személyes adatok alapjogi védelmét vette figyelembe, hanem az uniós trendeket és az Európa Tanács adatvédelmi ajánlásait is, így a magyar jog több ponton magasabb védelmet nyújtott a bizottsági javaslatnál (pl. tizenhat éves korhatár a szülői beleegyezéshez online szolgáltatások igénybevételekor – szemben a tizenhárom éves bizottsági javaslattal)[4].

A tagállamok álláspontját erősítette többek között az is, hogy kiszivárgott a Bizottság Jogi Szolgálata által készített szakvélemény, amelyben - egyebek mellett - arra mutattak rá, hogy az uniós jog egységessége nem kizárólag rendeleti formával érhető el.

Mivel azonban az Európai Parlament részéről a GDPR jelentéstevője informálisan világossá tette a Bizottságnak, hogy ragaszkodnak a

4 A GDPR végül azt a kompromisszumos megoldást vezette be, hogy a korhatár főszabály szerint tizenhat év, de a tagállamok ennél alacsonyabb, de tizenhárom évnél nem alacsonyabb korhatárt megállapíthatnak.

rendeleti formához, és Franciaország mellett időközben Németország is elfogadta azt, maradt ugyan a rendeleti forma, azonban az alapjogvédelem és az adatok szabad áramlása közötti egyensúly eredménye így összegezhető: az elfogadott GDPR olyan rendelet, amely tartalmában leginkább irányelv, mivel annak szövege több helyen igen tág megfogalmazású.

A tagállami parlamentekkel összefüggésben állandóan egy kiváló angol professzor, Philip Norton találó mondása jut eszembe, amely nagyjából így hangzik: a nemzeti parlamentek vagy megtanulnak az európai integrációval foglalkozni, és felülnek a brüsszeli gyorsra, vagy pedig lemaradnak. Először a Lisszaboni Szerződés rögzítette a nemzeti parlamentek arra való jogosultságát, hogy a szubszidiaritás elvének védelmében vizsgálhassák az uniós jogszabálytervezeteket. Az ellenőrzés lehet előzetes vagy utólagos, előbbi hatékonyságához több tagállam összefogása szükséges, az utóbbi pedig a Bíróság közreműködésével valósulhat meg.

Összességében elmondható, hogy a rendszer hatékonysági mutatója meglehetősen csekély, a tapasztalatok szerint csupán a legállhatatosabb tagállamok parlamentjének „sárgalapos figyelmeztetései" tudtak beavatkozni az uniós jogalkotás előkészítő szakaszába. Számos országban érezhető csalódottság amiatt, hogy vélt vagy valós hatáskörelvonás történt, és mégsem sikerült eredményesen befolyásolni az eseményeket. A nemzeti parlamentek másik szerepköre a Bizottsággal folytatott politikai párbeszéd, melynek keretében információt tudnak cserélni szakpolitikai kérdésekről, s így képviselethez jut a tagállamok kormányzati véleménye. Magyarországi példával élve fontos megemlítenem, hogy a terrorveszélyhelyzet bevezetése az Európai Bírósághoz fordulás eredményének következménye.

2. Az egyablakos mechanizmus

A másik koncepcionális aggály az egyablakos mechanizmussal (*one-stop shop*) kapcsolatban merült fel. A probléma lényege a következő:

Az akkor hatályos helyzethez képest a Bizottság eredeti javaslata szerint ugyanis mindössze annyi változott volna, hogy a Magyarországon lakó érintett a Facebookkal szembeni panaszát már nem kizárólag az ír adatvédelmi biztosnál nyújthatta volna be, hanem a magyar hatóságnál, a NAIH-nál is. A NAIH-nak viszont mindössze egy postáséhoz hasonló szerep jutott volna: eljuttatni a magyar panaszt az ír hatóságnak. (A panasz fordítási költségének kérdéséről a bizottsági javaslat hallgatott.) Így a panaszt továbbra is kizárólag az ír hatóság bírálta volna el. Ha pedig az ír hatóság ki is szabott volna bírságot a Facebookkal szemben, a határozatot továbbra is csak ír bíróság előtt lehetett volna megtámadni, és a magyar adatalany továbbra is legfeljebb azt indítványozhatta volna az ír bírónál – ír ügyvéd igénybevételével –, hogy forduljon az Európai Unió Bíróságához előzetes döntéshozatali eljárás keretében.

2013 decembere kapcsán kiemelést érdemel, hogy a Tanács Jogi Szolgálatának főigazgatója, aki korábban bíró volt az Európai Unió Bíróságán (M. Hubert Legal), mutatott rá a 2013. decemberi BIÜT-ön, hogy a Bizottság alapjogokért felelős biztosa által jegyzett egyablakos mechanizmus-koncepciója sérti az Unió Alapjogi Chartáját, mert egy uniós alapjog megsértése esetére nem biztosítja az adatalany számára a hatékony jogorvoslat lehetőségét egyetlen uniós (pl. Európai Unió Bírósága) fórum előtt sem. Ezért reális a veszélye annak, hogy ez a koncepció, amennyiben a GDPR elfogadásra kerülne, elbukna az Európai Unió Bírósága előtt.

Mivel a GDPR-t jegyző Reding biztos ragaszkodott az egyablakos mechanizmus eredeti koncepciójához, a Tanácsban csak más, kisebb kérdésekben lehetett előrehaladást elérni.

Így 2014 márciusában, 2014 decemberében és 2015 márciusában a BIÜT (csak) részleges általános megközelítést tudott elérni a GDPR más fejezeteiről.

2015 tavaszán a GDPR egyik központi elemét jelentő egyablakos mechanizmus kapcsán végül az új, Juncker-bizottság és az adatvédelemért felelős új igazságügyi biztos, Vera Jourová személye hozott áttörést, illetve valószínűleg az, hogy ekkor már egyre több helyen lehetett arról hallani Brüsszelben, hogy a tagállamok ellenállása miatt zátonyra futhat az egész adatvédelmi reform.

A kompromisszum eredményét most egy példán szemléltetem:

Ha ma egy Magyarországon lakó adatalany úgy ítéli meg, hogy pl. a Facebook GDPR-ba ütközően kezelte valamely személyes adatát, akkor két lehetősége van:

- Az egyik új lehetőség szerint a NAIH-hoz nyújthatja be panaszát anyanyelvén, aki azt továbbítani köteles az ír adatvédelmi hatóságnak; szintén nóvum, hogy a panasszal nem foglalkozó bármelyik hatósággal szemben közvetlenül bírósághoz lehet fordulni; a panasz elbírálása során a magyar és az ír hatóság együttműködni köteles azzal, hogy az „első fokú" határozatot az ír hatóság, mint fő hatóság fogja meghozni. Ha az ír döntéstervezettel a NAIH nem ért egyet, akkor az Európai Adatvédelmi Testülethez mint másodfokú hatósághoz fordulhat, kérve az ügy elvi eldöntését (pl. volt-e jogellenes adatkezelés vagy sem). Az Európai Adatvédelmi Testület ekkor kötelező erejű döntést bocsát ki – az egységes uniós jog előmozdítása érdekében –, és az ír hatóság a Testület döntésével összhangban köteles meghozni saját határozatát. Ezt az ír határozatot továbbra is meg lehet támadni ír bíróság előtt, amelynek során kérelmezni lehet előzetes döntéshozatalt az Európai Bíróságtól.
- A másik, szintén új jogorvoslati út szerint a Magyarországon tartózkodó adatalany közvetlenül magyar bíróság előtt indíthat keresetet a Facebookkal szemben.

Bármelyik jogorvoslati utat is veszi igénybe az adatalany, lényeges elem, hogy ilyenkor a végső döntés – előzetes döntéshozatali eljárás révén – mindig az Európai Unió Bíróságának a kezében van.

A folyamatok lezárásaképpen végül 2015 júniusában a Tanács bel- és igazságügyi formációjában, miután a Bizottság nyitott lett a Tanács Jogi Szolgálata által felvetett uniós alapjogi aggályok orvoslására, felgyorsultak a tárgyalások. Ennek eredményeképpen a 2015. júniusi BIÜT általános megközelítést ért el a GDPR valamennyi fejezetéről, lezárva ezzel az első olvasatos eljárást, megnyitva egyúttal az utat a Tanács, a Parlament és a Bizottság közötti trialógus tárgyalások megkezdése előtt.

VI. Az Európai Parlament

Az Európai Parlament kezdettől fogva támogatta az adatvédelmi reformot. Sőt, az EP nyomására döntött úgy a Bizottság, hogy bevonja a reformba a 2008-ban elfogadott bűnügyi adatok továbbítását szabályozó kerethatározatot annak ellenére, hogy azt több tagállam még nem is implementálta 2012-ig. Ezért nyújtotta be a Bizottság a GDPR mellett a bűnügyi személyes adatokkal kapcsolatos irányelvtervezetet.

A két tervezetet az alapjogokért is illetékes LIBE szakbizottság tárgyalta. A GDPR jelentéstevője Jan-Philipp Albrecht, a Zöldek képviselője lett. Árnyék-jelentéstevők voltak: Axel Voss (EPP), Marju Lauristin (S&D), Sophie in't Veld (ALDE), Timothy Kirkhope (ECR), Cornelia Ernst (GUE/NGL), Kristina Winberg (EFDD), Marine Le Pen (ENF). A nagy frakciók álláspontjai között koncepcionális, markáns különbségek nem voltak.

A bűnügyi irányelv jelentéstevője Marju Lauristin (S&D) volt, az árnyékjelentéstevők pedig Axel Voss (EPP), Sophie in't Veld (ALDE), Jan-Philipp Albrecht (Greens/EFA), Timothy Kirkhope (ECR), Cornelia Ernst (GUE/NGL), Kristina Winberg (EFDD)

Az EP tartotta magát a Bizottsággal megállapodott menetrendhez, mivel a LIBE szakbizottság már 2013 őszén szavazott a

kompromisszumos szövegekről, annak ellenére, hogy a GDPR-hoz több mint háromezer (!), az irányelvhez több mint ötszáz módosító javaslat érkezett, majd 2014 tavaszán le is zárta az első olvasatos eljárását.

Az EP – a Tanáccsal ellentétben – nem vitatta a rendeleti formát, sőt, a GDPR jelentéstevője többször jelezte, hogy a bűnügyi irányelvet is rendeleti formában kellene szabályozni. (A Tanácsban a tagállamok azért nem emeltek kifogást az irányelvvel szemben, mert az minimum harmonizációra törekszik, így a legtöbb nemzeti jogban nem hozott forradalmi változást).

VII. Az uniós adatvédelmi reformfolyamat lezárása

Miután 2015 júniusában a Tanács is lezárta az első olvasatos eljárását, fél év alatt sikerült minden vitás kérdést rendezni, így 2015. december 17-én a Tanács és az EP megállapodott a két javaslat végleges szövegéről. 2016. április 27-én formálisan elfogadta a Tanács és az EP a két jogszabályt

A GDPR-t 2016. május 4-én hirdették ki az Európai Unió Hivatalos Lapjában, és a kihirdetést követő huszadik napon lépett hatályba. (A bűnügyi irányelvet 2018. május 6-ig kellett a tagállamoknak átültetniük nemzeti jogukba.)

A GDPR-t 2018. május 25-től kell teljes egészében kötelezően és közvetlenül alkalmazni valamennyi EGT-tagállamban, így Norvégiában, Izlandon és Liechtensteinben, valamint Svájcban, amely ugyan nem tagja az Európai Gazdasági Térségnek, de az Unióval és a tagállamokkal kötött szerződés alapján a személyek szabad mozgása vonatkozásában azonos jogállású. Két EGT-tagállam és Svájc rendszeresen részt vett és többször hozzá is szólt a tanácsi szakértői szintű tárgyalások során.

Az Egyesült Államok hivatalosan nem nyilvánított véleményt az EU adatvédelmi reformjáról, de a Facebook, a Google és más amerikai technológiai vállalat-csoportok kezdetben szkeptikusan nyilatkoztak az uniós reformfolyamatról.

Ennek ellenére az elmúlt két évben annak lehettünk a tanúi, hogy az uniós adatvédelmi elvek és normák közül számos - legalábbis formálisan - importálásra került az amerikai jogba. Erre a formális jogimportra példa a 2016 júliusában elfogadott, az EU és az USA közötti kereskedelmi célú adatcserét szabályozó egyezmény (EU-USA Privacy Shield), amely a Schrems-ügyben hozott 2015-ös európai bírósági döntés[5] hatására újraírta a transzatlanti adatcsere feltételeit.

Meg kell azonban jegyezni, hogy az uniós adatvédelem amerikai átvételéről azért még korai lenne beszélni, például azért, mert 2018 júliusában egy ír fellebbviteli bíró az Európai Unió Bíróságához fordult többek között annak eldöntését kérve, hogy a perben érintett amerikai vállalat ír leányvállalata által végzett transzatlanti adatcsere-gyakorlat és az új EU-USA adatcsere egyezmény sérti-e a személyes adatok védelméhez való uniós alapjogot, vagy sem.[6]

5 C-362/14 Maximillian Schrems v Data Protection Commissioner

6 C-311/18 Facebook Ireland és Schrems. 2018. május 9-én kelt előzetes döntéshozatali kérelem, folyamatban lévő ügy

Dr. Salgó László Péter[1]

A magyar GDPR-megfelelés jogalkotási eredményei és kérdések a jövőre nézve

A személyes adatok védelméhez való jog – melyet az Alaptörvény VI. cikkének (3) bekezdése garantál – az alapjogok harmadik generációjának individuális szabadságjoga. Harmadik generációs alapjog, mivel a XX. század második felétől jelentkezett a szükség alapjogként való elismerésére a különböző technikai, technológiai vívmányok hatására. Ezen alapjog erőteljes személyhez kötöttségét mi sem bizonyítja jobban, mint az, hogy hazánkban az egyik nevesített személyiségi jogként a polgári jog is védelemben részesíti, megsértése esetén akár sérelemdíj vagy kártérítés megállapítását is előirányozva.[2] Ezen alapjog a magyar Alkotmánybíróság több határozatának is tárgya volt, melyben e jog intézményvédelmi oldalának szerepe is kirajzolódott, így a jogalkotó pozitív jogalkotási kötelezettségének fontossága e jog védelme tekintetében szintén nagy szerephez jutott.

Az első ilyen, a személyes adatok védelméhez való jog alapjogi dogmatikájának megalapozásában kiemelt szerepet betöltő alkotmánybírósági határozat az 15/1991. (IV.13.) AB határozat volt. Az Alkotmánybíróság e határozatában kimondta a korlátozás nélkül használható, általános és egységes személyazonosító kód alkotmányellenességét.

Az Alkotmánybíróság ebben a határozatában kifejtette, hogy *„a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként*

1 Jogszabály-előkészítés összehangolásáért és közjogi jogalkotásért felelős helyettes államtitkár, Igazságügyi Minisztérium

2 A Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) 2:43. § e) pontja, 2:51-2:53. §

értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként." Ezen alapjog tartalma az Alkotmánybíróság értelmezése szerint az, „*hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.*" Alapelvként kell érvényre juttatni a személyes adatok kezelése során a célhoz kötöttség elve mellett az adattovábbítás és az adatok nyilvánosságra hozásának korlátozására vonatkozó alapelveket is.[3]

Az Alaptörvény VI. cikke rendelkezik a személyes adatok védelmére vonatkozó szabályokról. Ezen cikk generálisan is védelemben részesíti a személyes adatok védelmét, továbbá előírása szerint védelme felett egy, sarkalatos törvényben létrehozott független hatóság őrködik.[4] Az alapvető jogokra vonatkozó szabályokat törvényi szinten szükséges megállapítani,[5] a személyes adatok védelméhez, valamint a közérdekű adatok megismeréséhez való jog érvényesülésének általánosságban érvényre juttatandó részletes szabályait az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) tartalmazza. A személyes adatok védelméhez való jog azonban nem korlátozhatatlan, azaz abszolút védelemben részesülő alapjog. Az úgynevezett „szükségességi-arányossági" teszt alapján a személyes adatok védelméhez való jog korlátozható, amennyiben felmutatható egy olyan legitim cél (másik alapvető jog, valamely alkotmányos érték), mely az alapjogkorlátozást szükségessé teszi. Vizsgálni szükséges továbbá, alkalmas-e az igénybe vett eszköz a legitim cél eléréséhez, szükséges-e, azaz nem áll-e rendelkezésre más eszköz a cél

3 15/1991. (IV.13.) AB határozat
4 Magyarország Alaptörvénye VI. cikk (3)-(4) bekezdése
5 Magyarország Alaptörvénye I. cikk (3) bekezdése

elérése érdekében, az ezzel okozott jogsérelem pedig arányban áll-e az elérendő céllal.[6]

A személyes adatok védelméhez való jog rövid jellemzését követően, a következőkben a jogalkotó szerepét, illetve feladatait ismertetem Magyarország európai uniós tagállami kötelezettsége vonatkozásában.

E rövid bevezetés azért volt szükséges, mert az Alaptörvény mint a jogrendszerünk alapja az európai uniós jogi szabályozástól de facto függetlenül határozta, illetve határozza meg a személyes adatok védelmére vonatkozó alkotmányos szabályokat, követelményeket. Tehát a szabályozás alapja állandó, viszont a szabályozás tartalmában jelentős változások történtek.

I. A személyes adatok védelmére vonatkozó uniós szabályozás 2018. május 25-e előtt

Magyarország 2004. május 1-je óta az Európai Unió tagja, a hazai jogalkotást pedig az uniós tagságunk óta áthatják az európai uniós jogalkotás során elfogadott uniós jogi aktusok. Nem jelent kivételt ez alól a személyes adatok védelmének területe sem. Az Európai Unió Működéséről szóló Szerződés 16. cikke deklarálja, hogy mindenkinek joga van személyes adatainak védelméhez, az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében szabályokat állapít meg e védelem biztosítása érdekében.[7]

2018. május 25-éig az információs önrendelkezési jogot érintő szabályokat „kódex" jelleggel az Infotv. tartalmazta. Ennek oka az volt, hogy az uniós jogalkotó elsősorban átültetést igénylő normák elfogadásával harmonizálta a tagállamok eltérő szabályait a személyes adatok védelme területén. E jogharmonizációs feladatot *a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok*

6 Magyarország Alaptörvényének I. cikke
7 Ld. EUMSZ 16. cikk

szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv (általános adatvédelmi irányelv), *az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv),* továbbá *a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló, 2008. november 27-i 2008/977/IB kerethatározat* töltötte be. Az irányelv olyan uniós jogi aktus, mely a kötelezően elérendő célokat határozza meg a címzett tagállamok számára, azonban a megvalósítás eszközei a tagállamok számára szabadon meghatározhatóak,[8] a kerethatározat hasonló funkcióval bíró uniós jogforrás. Az irányelvet a tagállamok kötelesek átültetni a jogrendszerükbe és az abban meghatározott célt végrehajtani. Amennyiben valamely tagállam nem tesz eleget egy irányelv átültetését igénylő kötelezettségének, a Bizottság kötelezettségszegési eljárást indíthat.[9]

Amint látható, 2018. május 25-éig a személyes adatok védelme területén a jogharmonizáció eszközét alkalmazta az uniós jogalkotó, és a Magyarországon alkalmazandó személyes adatok védelmére vonatkozó szabályokat az Infotv. határozta meg. 2018. május 25-e után azonban jelentős változásoknak lehettek tanúi az uniós polgárok.

II. A személyes adatok védelmére vonatkozó uniós szabályozás 2018. május 25-e után

Az Európai Unióban 2012-ben megkezdett, a személyes adatok védelmét érintő jogalkotási folyamat eredményeképp a Tanács és az Európai Parlament mint társjogalkotók 2016-ban két jogalkotási aktus elfogadásáról döntöttek az adatvédelem terén, egyrészt *a természetes*

8 Ld. EUMSZ 288. cikk
9 Ld. EUMSZ 260. cikk (3) bekezdés

személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletről (a továbbiakban: általános adatvédelmi rendelet), másrészt *a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelvről* (a továbbiakban: Irányelv).

Az Európai Bizottság az adatvédelmi reform szükségességét a gyors technológiai fejlődéssel, valamint a globalizáció által előidézett új kihívásokkal indokolta. A személyes adatok (jellemzően elektronikus úton történő) tömeges kezelése és az erre épülő üzleti modellek fokozottan veszélyeztetik az egyének személyes adataik védelméhez fűződő jogainak érvényesülését, ezért indokolttá teszik azok megerősítését. Emellett a korábbi, irányelvre épülő tagállami normák helyébe lépő, uniós szinten egységesített jogi szabályozásnak köszönhetően – a Bizottság véleménye és számításai szerint – csökkenhetnek a tetemes adminisztratív költségek, és ez évente több mint kétmilliárd eurós megtakarítást jelenthet majd a vállalkozásoknak.

Az elfogadott rendelet 2016. május 4-én jelent meg az Európai Unió Hivatalos Lapjában és 2018. május 25-től minden tagállamban kötelező alkalmazni. Megjegyzendő, hogy a rendelet elfogadását megelőző hatályos magyar jogszabályi környezet a személyes adatok védelmének az Európai Unió tagállamai között az egyik legmagasabb védelmi szintjét biztosította, így Magyarország Kormánya az uniós rendelet tárgyalása során fenntartotta azon álláspontját, hogy az új európai uniós adatvédelmi szabályozás ne rendeleti, vagyis közvetlenül alkalmazandó uniós aktus formájában, hanem irányelvi, vagyis tagállami mozgásteret

biztosító, átültetést igénylő jogforrásban kerüljön megalkotásra.[10] Az uniós intézmények és a tagállamok többsége azonban arra törekedett, hogy az Európai Unió területén egységes, közvetlenül alkalmazandó szabályösszesség kerüljön kidolgozásra, és csak a bűnüldözési célú adatkezelés területén maradjon meg az irányelvi jogforrási szint. Megjegyzendő továbbá, hogy a Bizottság véleménye szerint az egységes szabályozással el lehet kerülni, hogy egyes multinacionális nagyvállalatok a tagállamok eltérő adatvédelmi rezsimjeit kijátszva a számukra legkedvezőbb szabályokat biztosító országokban folytassák adatkezelési tevékenységüket.

Az Általános adatvédelmi rendelet 2. cikkének (2) bekezdése szól a rendelet tárgyi hatályáról és határozza meg azon területeket, melyeken az általános adatvédelmi rendelet előírásai nem érvényesülnek. Az általános adatvédelmi rendelet tárgyi hatálya általánosan személyes adatok részben vagy egészben automatizált, illetve nem automatizált módon történő kezelésére terjed ki, abban az esetben, ha a személyes adatok nyilvántartási rendszer részét képezik, vagy annak részévé kívánják tenni.[11] A rendelet tárgyi hatályán kívül esnek az uniós jog hatályán kívül eső tevékenységek során történő személyes adatkezelések, ide tartozik elsősorban a honvédelem, nemzetbiztonság területe, mely a tagállamok szuverenitásának teljes körű tiszteletben tartásával a tagállamok kizárólagos szabályozási kompetenciájába tartozik. Szintén kivett esetkört képeznek a közös kül- és biztonságpolitika területén történő személyes adatkezelési műveletek, valamint a kizárólag személyes vagy otthoni tevékenység keretében végzett adatkezelés is. A rendelet hatálya nem terjed ki azon adatkezelésekre sem, amelyet az Irányelv szabályoz. Szükséges végül kiemelni, hogy a rendelet hatálya nem terjed ki a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek által végzett adatkezelési műveletekre sem, hiszen ilyen típusú

10 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról szóló 2018. évi XIII. törvényhez fűzött indokolás, http://www.parlament.hu/irom41/00335/00335.pdf

11 Általános adatvédelmi rendelet (GDPR) 2. cikk (1) bekezdése

adatkezelésekre a *45/2001/EK rendelet* (valamint a nemsokára hatályba lépő új intézményi adatvédelmi rendelet) alkalmazandó.[12]

A bűnüldözési célú adatkezelések esetében a Bizottság indokoltnak találta az irányelvi szint fenntartását, tekintettel arra, hogy e területen különös szabályok szükségesek.[13] Az Irányelvet a tagállamoknak 2018. május 6-áig kellett átültetniük.[14]

Szükséges néhány szót szólni a személyes adatok kezelését érintő, folyamatban lévő európai uniós jogi aktusokról is. *A természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről szóló, 2018. október 23-i (EU) 2018/1725 európai parlamenti és a tanácsi rendelet* elfogadásával az európai unió intézményeinek adatkezelése is az általános adatvédelmi rendelet adta rezsimhez igazodik, az elektronikus hírközlés területén szintén a korábbi jogharmonizáció eszközét jelentő irányelv helyett rendeleti szintű szabályok kerülhetnek elfogadásra (*e-privacy rendelet*).

A személyes adatok védelméhez való jogot érintő uniós jogi aktusok áttekintését követően, a következőkben kifejezetten a magyar jogalkotó lépéseit ismertetem, melyek az elfogadott uniós jogi aktusokra való reakcióként születtek.

III. A magyar jogalkotást érintő feladatok

A magyar jogalkotóra az új uniós adatvédelmi rezsim aktusok elfogadását követően több feladat is várt. Az Igazságügyi Minisztériumnak – mint jogszabály-előkészítőnek – azt kellett eldöntenie, hogy a két aktust milyen módon ülteti át és hajtja végre. E folyamat kezdetén

12 Általános adatvédelmi rendelet 2. cikk (GDPR) (2)-(3) bekezdése
13 Irányelv (Police Directive) preambulum (10) bekezdése
14 Irányelv (Police Directive) 63. cikk (1) bekezdése

elvi döntés született arról, hogy az elfogadott új uniós jogi aktusokat az *Infotv.* módosításával fogja átültetni és végrehajtani a magyar jogalkotó.

Az Infotv. átfogó felülvizsgálata folyamán egyrészről meg kellett vizsgálni, hogy az Infotv. rendelkezései mennyiben egyeztethetőek össze az általános adatvédelmi rendelet rendelkezéseivel, továbbá, hogy az Irányelv átültetése milyen szerkezeti módosításokat igényel az Infotv. szövegében. A jogszabály-előkészítő munka eredményeként 2017 őszén jelent meg az általános adatvédelmi rendelettel való összhang megteremtése, valamint az Irányelv átültetése érdekében az Infotv. módosításáról szóló jogszabálytervezetet, amelyet a Kormány társadalmi egyeztetésre is bocsátott. A társadalmi egyeztetést nagyfokú együttműködés jellemezte a stratégiai partnerekkel, melynek köszönhetően 2018 tavaszán a tényleges jogalkotási folyamat megkezdődött. Az eredeti koncepció helyett két csomagra bontva kerültek benyújtásra a szükséges módosítások, egyrészről az úgynevezett „rövid csomag", másrészről pedig egy úgynevezett „hosszú csomag" útján.

IV. A „rövid csomag"

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról szóló 2018. évi XIII. törvény kijelölte a Nemzeti Adatvédelmi és Információszabadság Hatóságot (a továbbiakban: NAIH) az általános adatvédelmi rendelet szerinti független felügyeleti hatóságokra[15] vonatkozó feladatok ellátására, összhangban az *Alaptörvény* VI. cikkének (4) bekezdésével (megjegyzem, hogy az alaptörvényi szabályok alapján, a jelenlegi magyar jogrendszerben más jogi lehetőség nem is lett volna, mert az Alaptörvényből és az Infotv.-ből most is következik, hogy egy magyar adatvédelmi hatóság van, és az a NAIH). A rendelet e cikke a személyes adatok védelméhez való jog legteljesebb érvényesülésének biztosítása

15 Általános adatvédelmi rendelet (GDPR) 51. cikke

érdekében egy sarkalatos törvényben létrehozandó hatóságnak a követelményét fogalmazza meg a személyes adatok kezelésére vonatkozó jogszabályi előírások betartásának ellenőrzése céljából. A NAIH hatáskörrel való felhatalmazásáról szóló szabályok elfogadására égető szükség volt, hiszen a korábbi rendelkezések alapján a NAIH már nem indíthatott hatósági eljárást az általános adatvédelmi rendelet alkalmazásának megkezdését követően.

Szintén a „rövid csomag" által került elfogadásra az Infotv. 75/A. §-ban meghatározott azon szabály is, amely szerint a NAIH a számára rendelkezésre álló hatásköröket az arányosság elvének figyelembevételével gyakorolja, amely azzal valósul meg, hogy a Hatóság a jogsértés első alkalmával elsősorban – az eset összes körülményére, így a jogsértés súlyára, annak ismétlődő jellegére, valamint az érintetti kör nagyságára is figyelemmel – az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik. A törvényjavaslathoz fűzött indokolás szerint a Kormány álláspontja, hogy a rendelet közvetlenül hatályosuló szabályait eredeti rendeltetésüknek megfelelően, vagyis elsősorban a tagállami jogrendszerek közötti különbséget kihasználó multinacionális gazdasági társaságok ellen fellépve szükséges alkalmazni, míg a többi gazdasági szereplő – elsősorban és kiemelten a kis- és középvállalkozások – tekintetében az arányosság elvét figyelembe véve a figyelmeztetés jogkövetkezményét indokolt alkalmazni. A jogalkotó tehát ezen szempontok figyelembe vétele érdekében a jogalkalmazót – azaz a NAIH-ot – „orientáló" szabályokat is meghatározott."[16] Ez amúgy nem egyedülálló, például az osztrák jogalkotó is hasonló szabályt fogalmazott meg.[17]

16 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról szóló 2018. évi XIII. törvényhez fűzött indokolás, http://www.parlament.hu/irom41/00335/00335.pdf (Utoljára megtekintve: 2018.12.04.)

17 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) 11. §

IV. A „hosszú csomag"

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvény célja az volt, hogy az *Irányelv* átültetéséhez, valamint az általános adatvédelmi rendelet végrehajtásához szükséges rendelkezések elfogadásra kerüljenek.

Az általános adatvédelmi rendelet végrehajtása kapcsán a magyar jogalkotó alapvető feladata az volt, hogy az Infotv. az általános adatvédelmi rendelettel ellentétes vagy azt megismétlő szabályokat ne tartalmazzon. Az általános adatvédelmi rendelettel ellentétes rendelkezést ugyanis a magyar jogalkotó nem tarthat fenn, továbbá tartózkodnia kell ilyenfajta jogalkotástól. A jogalkotót ugyanakkor pozitív jogalkotási kötelezettség is terhelte a rendelet végrehajtásának elősegítése érdekében. E pozitív jogalkotási kötelezettség elsősorban az anyagi jogi szabályokhoz kapcsolódó megfelelő intézményi és eljárásjogi keretek biztosítását jelentette, így különösen a NAIH kijelölését a „rövid csomagban", míg működése feltételeinek és eljárásrendjének biztosítását a „hosszú csomagban".[18]

Elmondható továbbá, hogy a rendelet számos ún. *nyitott,* vagy *rugalmassági klauzulát* tartalmaz, amely rendelkezések kifejezetten lehetőséget adnak a tagállamok számára, hogy az adott területen a rendelettől eltérő szabályokat alkossanak. Tipikusan ilyennek tekinthető az általános adatvédelmi rendelet 23. cikke, amely az érintetti jogok korlátozását teszi lehetővé.[19] A rugalmassági klauzulák speciális típusát jeleníti meg a rendelet IX. fejezete. E fejezet rendelkezik azon speciális területekről (személyes adatok kezelése és a véleménynyilvánítás

18 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvényhez fűzött indokolás, http://www.parlament.hu/irom41/00623/00623.pdf

19 Általános adatvédelmi rendelet 23. cikke

szabadságához és a tájékozódáshoz való jog viszonya, hivatalos dokumentumokhoz való nyilvános hozzáférés során történő adatkezelés, nemzeti azonosító számok kezelése, foglalkoztatással összefüggő adatkezelés, közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott adatkezelés, titoktartási kötelezettségek, egyházak és vallási szervezetek létező adatvédelmi szabályai), melyek esetében lehetséges, vagy akár kifejezetten szükséges is a rendelet meghatározott rendelkezéseitől való eltérés, illetve az azt pontosító szabályok elfogadása.[20] Megemlítendő, hogy a rendelet több esetben értesítési kötelezettséget (speciális notifikáció) is telepít a tagállamokra az ezzel összefüggésben elfogadott (valamint módosított) rendelkezések vonatkozásában. Magyarország augusztus 1-jén teljesítette e notifikációs kötelezettségét a Bizottság felé a Hatóság függetlenségét biztosító, a szankcionálásra vonatkozó, a véleménynyilvánítás szabadsága és a személyes adatok védelme összeegyeztethetőségét biztosító, valamint a foglalkoztatásra és a titoktartási kötelezettségekre vonatkozó szabályokról.[21]

A megváltozott jogszabályi környezet alapján a jogalkalmazónak első lépésként azt kell eldöntenie, hogy az adott adatkezelési jogviszony az általános adatvédelmi rendelet tárgyi hatálya alá tartozik-e, avagy sem. Abban az esetben, ha az adatkezelési jogviszonyban a rendelet alkalmazandó, a jogalkalmazónak elsődlegesen a rendelet szabályaira kell figyelemmel lennie, emellett pedig az *Infotv.* 2. § (2) bekezdésében felsorolt rendelkezések az általános adatvédelmi rendeletet kiegészítő szabályként érvényesülnek. Az *Infotv*. 2. § (3) bekezdése egyértelművé teszi továbbá, hogy a bűnüldözési célú adatkezelésre, továbbá a nemzetbiztonsági, a honvédelmi célú adatkezelésre kizárólag az *Infotv.* rendelkezései vonatkoznak, így ezen adatkezelések esetében az Infotv. megőrzi „kódex" jellegét. Amennyiben az adatkezelés nem tartozik a

20 Voigt, P., von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer International Publishing AG, Switzerland.

21 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en (Utoljára megtekintve: 2018.12.04.)

fentiek közül egyik alá sem, az Infotv. visszautaló szabállyal határozza meg az általános adatvédelmi rendeletben alkalmazandó szabályok körét.[22]

A*z általános adatvédelmi rendelet* 6. cikk (1) bekezdésének c) és e) pontja az adatkezelés lehetséges jogalapjai között sorolja fel azon eseteket, amikor az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges vagy az adatkezelőre ruházott közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladatának végrehajtásához szükséges. E jogalapok tekintetében az általános adatvédelmi rendelet 6. cikk (2)-(3) bekezdése kifejezetten a tagállamokra telepíti azon „kiigazító" szabályok elfogadását, amelyek az ezen jogalapok keretében végzett adatkezelési követelményeket meghatározzák. Tekintettel arra, hogy a kötelező adatkezelés esetkörét az *Infotv.* már az általános adatvédelmi rendelet megszületése előtt is tartalmazta, a jogalkotó indokoltnak tartotta a kötelező adatkezelés jogintézményének fenntartását. Az *Infotv.* 5. § (3) bekezdése ezzel összefüggésben kimondja, hogy az általános adatvédelmi rendelet 6. cikk (1) bekezdés c) és e) pontja szerinti jogalapok tekintetében az adatkezelés kötelező adatkezelés keretében rendelhető el, és az ezt elrendelő törvényben, illetve önkormányzati rendeletben rendelkezni kell a kezelendő adatok köréről, az adatkezelés céljáról, feltételeiről, az adatok megismerhetőségéről, az adatkezelő személyéről, továbbá emellett rendelkezni kell a kötelező adatkezelés időtartamáról is.

Új jogintézményként jelenik meg az Infotv. rendszerében az adatkezelés szükségességének felülvizsgálata, amely szerint a kötelező adatkezelés időtartama a korábbiaktól eltérően immáron az adatkezelés szükségességének felülvizsgálatával is meghatározható. Amennyiben a jogalkotó tehát arról rendelkezik, hogy konkrét adatkezelési időtartam helyett az adatkezelés szükségességének felülvizsgálatát kell elvégezni, úgy az adatkezelőnek a kötelező adatkezelést elrendelő normában meghatározott időközönként felül kell vizsgálnia az adatkezelés

22 Infotv. 2. § (4) bekezdése

szükségességét. Amennyiben az adatkezelés időtartamára vonatkozóan nem található a törvényben, illetve önkormányzati rendeletben rendelkezés, az adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, szükséges-e a személyes adat kezelése az adatkezelés céljának megvalósulásához. Az adatkezelés szükségessége felülvizsgálata eredményét dokumentálni és tíz évig megőrizni köteles az adatkezelő, valamint a NAIH kérésére azt a NAIH rendelkezésére is kell bocsátania.[23]

Az *Infotv*. új, VI/A. fejezetében kaptak helyet a bírósági adatkezelési műveletek ellenőrzésére vonatkozó rendelkezések is. Az általános adatvédelmi rendelet 55. cikkének (3) bekezdése általános érvénnyel kimondja, hogy a tagállami felügyeleti hatóságok hatásköre nem terjed ki a bíróságok által igazságügyi feladataik ellátása során végzett adatkezelési műveletek felügyeletére.[24] Az általános adatvédelmi rendelet preambuluma szintén kifejti, hogy a bíróságok és más igazságügyi hatóságok tevékenységeire is alkalmazni kell a rendeletet, azonban a tagállamok, illetve az uniós jog e területen végzett adatkezeléseket részletesebben is meghatározhatják. E szabályozási modell oka, hogy a bírói kar függetlensége olyan alkotmányos jelentőségű, hogy a felügyeleti hatóságok hatásköre nem terjedhet ki olyan személyes adatok kezelésére, amelyet a bíróságok igazságszolgáltatási feladatkörükben eljárva végeznek.[25] Annak érdekében, hogy a bíróságok igazságszolgáltatási feladatkörében végzett adatkezelések esetében is alkalmazhatóak legyenek az általános adatvédelmi rendelet előírásai, a jogalkotó az ún. *adatvédelmi kifogás* jogintézményének bevezetéséről döntött. Az adatvédelmi kifogás intézményét az Igazságügyi Minisztérium a NAIH-val, a Kúriával és az Országos Bírósági Hivatallal együttműködve készítette elő, amelynek célja, hogy a bírósági döntés meghozatalára irányuló peres és nemperes eljárásokban, az azokra vonatkozó előírások alapján a bíróságok által végzett adatkezelési műveletekkel kapcsolatban is

23 Infotv. 5. § (3) és (5) bekezdése

24 Általános adatvédelmi rendelet (GDPR) 55. cikkének (3) bekezdése

25 Általános adatvédelmi rendelet (GDPR) preambulum (20) bekezdése

megvalósulhasson a személyes adatok védelméhez való jog érvényesülésének ellenőrzése. A kifogást az alapügyben eljáró bíróságnál kell benyújtani és a kifogás alapján a bíróságnak azt szükséges vizsgálnia, hogy az eljáró bíró, ülnök, igazságügyi alkalmazott az adatkezelési tevékenysége során a személyes adatok védelmére vonatkozó jogszabályi és uniós jogi előírásoknak megfelelően járt-e el.[26] Az adatvédelmi kifogás az eljárási kódexekben már alkalmazott más előterjeszthető kifogásokhoz hasonlóan szabályozott, ekként a nem orvosolható jogsértés esetén a bíróság megállapítja a személyes adatok jogellenes kezelésének tényét, míg orvosolható jogsértés esetén a bíróság reparatív jellegű jogkövetkezményeket ír elő, így például elrendelheti a jogellenes adatkezelési művelet megszüntetését, a jogellenes adatkezelés közvetlen veszélyének elhárítását, az adatkezelés jogszerűségének helyreállítását.[27] Amennyiben a jogsérelem orvoslására adatvédelmi kifogás nem kerül benyújtásra, az érintett a jogsérelem orvoslása iránt más eszközökkel is élhet, ekként különösen az Infotv. 23. §-a szerint bírósághoz fordulhat és kártérítést is követelhet az adatkezelőtől.

Szükséges kiemelni, hogy az általános adatvédelmi rendelet 35. cikkének (10) bekezdése szerint, ha a 6. cikk (1) bekezdés c) vagy e) pontja szerinti adatkezelés jogalapját uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot, úgy adatvédelmi hatásvizsgálatot az adatkezelőnek már nem szükséges készítenie. Az Infotv. 25/G. § (6) bekezdése ennek megfelelően a kötelező adatkezelések tekintetében a kötelező adatkezelést elrendelő jogszabály előkészítőjére telepíti az *adatvédelmi hatásvizsgálat* lefolytatását. Az adatvédelmi hatásvizsgálat lefolytatásának kötelezettsége tehát a kötelező adatkezeléssel elrendelt adatkezelések esetében a jogszabály

26 Infotv. 71/A. § (3) bekezdése és 71/B. § (1) bekezdése

27 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvényhez fűzött indokolás, http://www.parlament.hu/irom41/00623/00623.pdf

előkészítőjét terheli, nem az adatkezelőt. Szintén megjegyzendő, hogy a NAIH közzétette honlapján azon adatkezelési műveletekről szóló listáját, melyek esetében kötelező adatvédelmi hatásvizsgálat lefolytatása, felhívva emellett a figyelmet azonban arra is, hogy ezen adatkezelési műveleteken kívül más, az általános adatvédelmi rendelet 35. cikkének (1) és (3) bekezdésében meghatározott esetben (például nyilvános helyek nagymértékű, módszeres megfigyelése) is terheli az adatkezelőt az adatvédelmi hatásvizsgálat lefolytatásának kötelezettsége. A huszonnégy pontból álló közétett lista szerint többek között biometrikus adatok kezelésének módszeres megfigyelése, hitelképesség értékelése, profilozás esetén a NAIH szükségesnek tartja minden esetben adatvédelmi hatásvizsgálat lefolytatását.[28] A NAIH által közzétett lista mindamellett nem csupán az adatkezelő, hanem a jogalkotó számára is – az Infotv. 25/G. § (6) bekezdése szerinti esetben – kötelező.

Végül, de nem utolsó sorban szintén a csomag elfogadásának eredményeként, az Infotv. 72. § (3) bekezdésében kapott felhatalmazás alapján kiadásra került az Infotv. 34/A. alcímében szabályozott adatkezelési engedélyezési eljárásokhoz kapcsolódó igazgatási díjak mértékét szabályozó, *az adatkezelési engedélyezési eljárás lefolytatásáért fizetendő igazgatási szolgáltatási díjról szóló 25/2018 (IX.3.) IM rendelet* is. E rendelet részletesen szabályozza a fizetendő díjak mértékét, valamint a hatóság függetlenségével összhangban rögzíti, hogy az így beszedett díj a hatóság bevételét képezi.

V. A Személyes adatkezelés az ágazati törvényekben

Az általános adatvédelmi rendelet elfogadásával az adatkezelési jogalapok széles palettája nyílt meg az adatkezelők számára. Korábban, az Infotv. szabályai alapján személyes adat kezelésére az érintettől

28 https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf (Utoljára megtekintve: 2018.12.05.)

származó hozzájárulás, kötelező adatkezelés, valamint – a hozzájárulás beszerezhetetlensége esetén – az adatkezelőt terhelő jogi kötelezettség vagy érdekmérlegelésen alapuló jogos érdek alapján kerülhetett sor. Elmondható, hogy az ágazati joganyagban legfőképpen tehát – szükségszerűen – a kötelező adatkezelés dominált, ekként szinte minden ágazati törvényben megtalálható valamilyen az adatkezelést elrendelő vagy lehetővé tevő szabály.

Az általános adatvédelmi rendelet 6. cikkének (1) bekezdése ezzel szemben hat jogalapot említ, és e jogalapok tekintetében is több alapvető változást is hozott a rendelet alkalmazásának megkezdése. Bár a fentiekben említettek szerint a kötelező adatkezelések esetköre fenntartható maradt az általános adatvédelmi rendelet alkalmazása mellett is, fontos megjegyezni, hogy a kötelező adatkezelés mögött meghúzódó jogalapok egyértelműen jogi kötelezettséget vagy valamilyen közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtását tételeznek fel, ekként a jogalkotó mozgástere is nagymértékben szűkült a kötelező adatkezelések elrendelése terén.

A kötelező adatkezelésen kívüli jogalapok tekintetében a tagállami jogalkotó az adatkezelésre vonatkozó további feltételeket és jogokat nem állapíthat meg, ekként nem írhat elő többletfeltételeket a tagállami jogalkotó egy, az adatkezelő és az érintett között létrejött magánjogi, szerződéses jogviszony tekintetében, és ugyancsak nem határozhatja meg az adatkezelési jogviszony tartalmát a jogalkotó egy, az adatkezelő vagy harmadik személy jogos érdekén alapuló adatkezelés tekintetében sem. Ezen adatkezelési jogviszonyok esetén az adatkezelő felelőssége, hogy az adatkezelés céljait, az érintettek körét, a megőrzési időt meghatározza, ekként az ezen a jogalapon nyugvó adatkezelési jogviszonyok esetében a fennálló törvényi szabályok deregulációja szükséges.

Az Igazságügyi Minisztérium már 2017 tavaszán megkezdte azt a kormányzati koordináló munkát, amelynek célja, hogy a minisztériumok a felelősségi körük mentén készítsék elő az ágazati jogszabályokra vonatkozó módosítási javaslatokat. Az Igazságügyi Minisztérium a

tárcáktól kapott javaslatok alapján az ágazati jogszabályok módosítását tartalmazó előterjesztést 2018 őszén széles körben társadalmi egyeztetésre bocsátotta. Az ágazati jogszabályokat módosító javaslat előreláthatólag 2019 tavaszán kerülhet benyújtásra, annak tartalma jelenleg is egyeztetés alatt áll a jogalkalmazók és a jogszabály-előkészítő között.

A GDPR jogalkotói nézőpontból

The GDPR from the Point of View of Application

Urszula Goral[1]

The Challenges of GDPR compliance in Poland – the point of view of the national Supervisory Authority

In Poland, the issue of the personal data protection was settled for the first time in 1997 – in Article 51 and 47 of the Constitution of the Republic of Poland of April 2, 1997 – and comprehensively – in the Act of August 29, 1997 on personal data protection, supplemented by legal acts, so called implementing regulations. In the Polish legal system, GIODO was the authority responsible for guarding the observance of data protection rights in the past twenty years.

On 25 of May, the old Data Protection Act was replaced by the New Act implementing the GDPR. Of course, we all know that according to European law the GDPR applies directly, but some aspects had to be regulated at the national level in the form of the national Data Protection Act.

The European data protection reform involved two legal acts (as a package): the GDPR and the less popular Directive 2016/680, the so-called Police Directive. These two pieces of legislation should have been implemented by May 2018; however, Poland is still one of the ten Member States that did not meet the deadline for the implementation of the latter Directive. That is why, to regulate data protection issues related to the so-called third pillar matters, the Polish legislator

1 Polish Personal Data Protection Office; Director of the International Cooperation and Education Department, Cardinal Stefan Wyszyński University, Warsaw

upheld some of the provisions of the previous Data Protection Act. The draft law implementing the Police Directive was approved by the Polish government in August (2018), but is still not subject to the parliamentary procedure and this stage of the legislative procedure has not been started yet. It means that in Poland we have mixed the previous and the current legislation in the field where the Directive should be implemented. It also means that there are several institutions in Poland, especially in the context of law enforcement, which should apply both frameworks while performing their tasks.

As regards the new Data Protection Act, it should be mentioned that the draft was presented by the Polish government in March 2018, adopted by the Parliament in May – the date when the Polish Data Protection Act entered into force is very significant – 25 May 2018. It means that the parliamentary procedure was very fast, sometimes without deeper discussions, but the Act was adopted on time.

As far as another element of the legislative package in Poland is concerned, to implement the GDPR the government decided to propose a draft of the huge act that introduced amendments to sectoral legislations. They just started to propose changes in September 2017, and the scope of these changes is getting wider and wider. This is probably then reason why this act has not yet been adopted. It is not difficult to find out that the main aim of law is to limit the application of the GDPR in Poland. Numerous ideas appeared and one of the examples was the exemption of the information obligation in the context of SMEs. The position presented by our data protection authority was that such proposal is not in line with the GDPR. A consultation was also held between the Polish government and the European Commission and finally this proposal was not introduced.

As for the sectoral legislation, there are major changes regarding labor law, banking law and insurance law. It is difficult to foresee when this draft legislation will be adopted. The lack of existence of this law is not such a big problem, as the GDPR applies directly in all these fields. In terms of principles, obligations, all seems to be clear. However, there

seems to be some misunderstanding by some of the data controllers in certain sectors. It looks like the GDPR left an impression that data protection is a completely new phenomenon. However, it is not. Data protection legislation has existed since 1997 in Poland and remains largely the same in terms of general principles or data controllers' obligations. The biggest challenge in this whole discussion is that the GDPR should be considered as evolution rather than revolution. Many obligations are similar to the former ones under the previous Directive 95/46.

As regards the Polish Data Protection Act adopted in May 2018, it mainly focuses on the status and powers of the data protection authority. One of the changes introduced by the Act is the change of the name of the authority. We are now called – as a supervisory authority – the Personal Data Protection Office, the name GIODO (Inspector General for Personal Data Protection) no longer exists. In addition, this Act provides for specific rules for procedures before the supervisory authority in line with the general powers foreseen by the GDPR.

The effect of the General Data Protection Regulation required the adaptation of local law to the new requirements. The Act includes, *inter alia*, details on appointing and notifying a Data Protection Officer (DPO), who shall be appointed by a controller or a processor on a mandatory or voluntary basis. The appointment of the DPO should be followed by notification of the appointment to the competent supervisory authority. Provisions also regulate issues concerning DPOs, e.g. the rules for providing their contact details. We also modified the scope of information provided, adopted to the general requirements.

The new Act provides the procedural rules for the adoption and approval of codes of conduct. I would like to stress that we have high hopes for the development of such norms. This is a new tool in our national system. We had some experience in this field, because under previous legislation we used to promote this concept in the form of codes of good practices. However, this solution was not legally binding. Now, under the GDPR, codes of conduct can be very crucial enforcement mechanisms.

The Act also implements the general rules for the certification mechanisms on the national level. The Polish legislator decided that certification shall be carried out by the competent certification bodies accredited by the national accreditation agency and at the same time by the data protection authority. As you can see, in Poland we have a mixed model, not only dedicated to certification bodies. The Act furthermore sets forth general rules for the obligation to notify data breaches or procedural rules for prior consultations.

As regards the activities of the Polish Data Protection Authority, one of our responsibilities was the publication of the list of the processing operations which require data protection impact assessment (DPIA). The Polish Data Protection Authority prepared and published a draft list of processing operations which are subject to mandatory DPIA. We published the first draft of the list in March for public consultation with the official list of the national (not transborder) operations being published (by law) within three months from 25 May.

We are also subject to review within the European Data Protection Board (EDPB) under the consistency mechanism. The Polish authority has already received the opinion from the EDPB and we have introduced some amendments to the initial list. After the completion of the procedure both national and transborder lists are ready to be finally published.

The Personal Data Protection Office of Poland has issued a series of guidelines to help ensuring compliance with the GDPR, including:

1. *"Personal Data Protection at Work. A Guide for Employers"*. The Guide explains how employers shall process personal data of job applicants and employees during the recruitment process and the entire employment period in compliance with the GDPR and indicates how they should approach certain problems. It includes, e.g., the following guidelines:

- The employer can request from a job applicant only the data to the collection of which it is authorized by law and which are necessary for making the decision on their employment;
- Excessive or 'just in case' data may not be collected in the recruitment process;
- It is not permitted to collect the data on potential applicants from social networks nor to draw up blacklists of job applicants;
- The employer shall not make nor store copies of employee's ID cards;
- Monitoring of phone calls or tracking private e-mails of employees is not allowed;
- The employer can monitor official e-mail correspondence of employees, but they must be informed thereof.

2. "*Personal Data Protection at Schools and Educational Institutions: A Guide*". The Guide addressed to school principals and directors of educational institutions contains updated advice on the processing of personal data of children, their parents and guardians, teachers. It describes how to use the GDPR provisions and sectoral legal acts in specific situations. The Guide includes for example the following advice:
   - Schools and educational institutions can publish the lists of admitted or non-admitted applicants only at their seat (publication on the school's website is prohibited);
   - Posting information containing personal data of students for the purpose of distinguishing them for special educational achievements on boards at the premises of school is allowed and does not require previous consent of student's guardian.

3. *The Guide* "*Personal Data Protection in Electoral Campaign*". It is addressed to all entities involved in the election process – not only candidates and their committees, but also institutions carrying out

elections and the voters. It indicates *inter alia* the main principles of personal data processing, the notions and definitions provided in the GDPR. It stresses the importance of the role of data controllers and indicates that at various stages of the electoral campaign different controllers are processing the data. A separate part of the Guide includes answers to FAQs on practical problems related to personal data processing for the purposes of the election.

4. *"Guidelines of the President of the Personal Data Protection Office on the Use of Video Surveillance"*. In these Guidelines, the permitted purposes for which video surveillance can be used, the rights of the persons subject to surveillance, and the controllers' obligations are discussed in a comprehensive manner. The Guidelines include also answers to FAQs and were subject to public consultation. Currently, the information received during the consultation is being analyzed, and following analysis the updated version of the Guidelines will be published to inform video surveillance operators in adapting to the applicable legal provisions, including the GDPR and national regulations.

Dr. Szabó Endre Győző[1]

A GDPR alkalmazásának kihívásai a magyar adatvédelmi hatóság szempontjából

Bevezetés

Az újdonság egy szervezet, de még inkább egy szervezetrendszer életében mindig kihívást jelent. Ha pedig harmincegy tagállam hatóságainak és az Európai Adatvédelmi Biztosnak kell egyszerre mozdulnia, akkor az különösen is nagy próbatétel.

2018. május 25-e fordulópontot jelent az Európai Unió, de bizonyosan a *privacy* (magánélet) globális védelme terén is. Ez a dátum valószínűleg az évek múltán elvégzett elemzéseink alapján is erőteljes választóvonalat jelent majd az adatvédelem területén. Az előttünk álló évek arra is választ adnak majd, hogy az intézményrendszert felkészülten érte-e a GDPR alkalmazása, és az új szabályrendszer valóban a *privacy* védelmének erősödéséhez vezetett-e.

Az Európai Unió jogának és a magyar jognak a kapcsolata

A magyar jog rengeteg szálon kapcsolódik az Európai Unió jogához. Önálló sok tekintetben, azonban a közös hatáskörgyakorlás révén az Európai Unió tagállamai kötelesek azokat a szabályokat betartani,

1 Elnökhelyettes, Nemzeti Adatvédelmi és Információszabadság Hatóság (Magyarország)

amelyeket az Európai Unió intézményei megalkotnak. A GDPR alkalmazásának egyik megtapasztalt kihívása önmagában annak megértése-megértetése, hogy az uniós rendelet egy közvetlenül alkalmazandó jogi norma, ami nem igényel tagállami átültetést. Idegenkedés tapasztalható azzal kapcsolatban, hogy tisztán hazai jogviszonyokban egy uniós jogalkotási aktusra kell alapozni egy-egy igény megfogalmazását vagy éppen az érintetti joggyakorlást. Általában még nagyobb nehézséget okoz annak elfogadtatása, hogy a magyar jogalkotónak félre kell tennie az uniós joggal ellentétes tartalmú magyar jogszabályt az uniós jog hatékony érvényesülése érdekében.

A Hatóság és a hatósági munkatársak felkészítése

Az adatvédelmi felügyeleti hatóságok, Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) felkészítése a GDPR alkalmazására összetett feladat volt. A NAIH az engedélyezett létszámbővítési keretben új kollégákat vett fel. Az új munkatársak kiválasztása, felvétele és betanítása a szervezetnek jelentős feladat, ami sok energiát és időt vesz igénybe, tehát rövidtávon a létszámbővülés mérsékelt hatékonyság-növekedéssel jár, de közép- és hosszú távon értelemszerűen jelentős kapacitás-bővülésen megy keresztül a magyar hatóság.

A változások között kell megemlítenünk, hogy a hatóságok munkájukat új nyelvi környezetben végzik, az együttműködés nyelve ugyanis az angol, és ennek eredményeként a tagállami hatóságok munkája is kétnyelvűvé vált. Már nem csak a nemzetközi kapcsolattartásért felelős szervezeti egységek munkatársai szembesülnek a két nyelven végzendő munkával, hanem a hatóságon belül egyre többen vesznek részt benne.

A GDPR alkalmazására való felkészülés a hatóság oldalán jelentős erőfeszítéseket igényelt, mindeközben az adatkezelők, a piaci szereplők is folyamatosan készültek a GDPR végrehajtására. Az adatvédelemben

járatos szakértőket a hatóság munkatársai között is igyekeztek verbuválni. A magyar hatóság is szembesült a piac igényeivel, és néhány munkatársat valóban sikerrel csábítottak át adatkezelőkhöz vagy ügyvédi irodákba. Bár Magyarországon is érezhető volt ez a jelenség, közel sem olyan mértékben, mint más államokban. Van olyan ország, ahol a helyi adatvédelmi hatóság nemzetközi kapcsolatokért és együttműködésért felelős szervezeti egységéről szó szerint mindenki távozott, teljesen kiürült, a nulláról kellett újra építeni.

Új eljárások

A GDPR az adatvédelem terén számos új anyagi szabályt és intézményt reformált meg, valamint újakat vezetett be. A rendelet azonban nem csak az anyagi jog terén jelent újítást, hanem új eljárásrendet is hoz. A tagállami életviszonyok terén is közvetlenül szabályoz, amikor például a hatóságok feladat- és hatáskörét egységesen határozza meg. A hagyományosan a tagállami jogalkotó feladatkörébe tartozó szabályozási tárgykörök közül az uniós jogalkotó többet közvetlenül maga rendez, élve a közös hatáskörgyakorlás eszközével. Új eljárásként jelenik meg a korábban csak sporadikusan létező adatvédelmi incidens bejelentési kötelezettség, továbbá a hatóságok közötti együttműködések különböző formái.

Adatvédelmi incidens bejelentése

A GDPR az adatvédelmi incidensek általános bejelentési kötelezettségét vezeti be. Nem várt, nem tervezett események megtörténte után keletkezik a bejelentési kötelezettség, amely minden adatkezelőt terhel. A bejelentéseket az adatvédelmi hatóságok fogadják. A magyar hatóságnál is fel kellett építeni a szoftveres környezetet, amely a bejelentési rendszernek a technikai hátterét adja, továbbá olyan szakértői hátteret

kellett kialakítani, amely ezt a feladatot el tudja látni. Ebben a csoportban jogászok és informatikusok együtt értékelik az incidens körülményeit. Megjegyezhetjük, hogy a bejelentések száma (napi egy-két incidens) egyelőre elmarad a korábbi várakozásoktól, de a szám az évek során várhatóan növekedni fog.

Egyablakos ügyintézés

Határon átnyúló adatkezeléseket érintő ügyek intézésében több hatóság vesz részt, vezető szerepet a tevékenységi központ szerinti adatvédelmi hatóság játszik. Azok a hatóságok, amelyekhez az adott ügyben panasszal fordultak, vagy ahol az adatkezelőnek letelepedési helye van, továbbá ahol az adatalanyok jelentős mértékben érintettek az adatkezelés által, az adatvédelmi hatóság úgynevezett érintett hatóságként kapcsolódik be az eljárásba. Jelentős beleszólása van az érintett hatóságoknak, az ő egyetértésük nélkül a vezető hatóság nem hozhatja meg végleges döntését. Amennyiben a résztvevő hatóságok között vita alakul ki, annak rendezése a Testület hatáskörébe tartozik.

Kölcsönös segítségnyújtás

Az együttműködésnek ez a formája kapcsolódhat az egyablakos ügyintézéshez és attól függetlenül is igénybe vehető. A hatóságok között a formalizált kölcsönös segítségnyújtástól függetlenül megmaradt a „régi", informális kölcsönös segítségnyújtás, ami önkéntes alapú.

A GDPR által szabályozott kölcsönös segítségnyújtásra a megkeresett hatóság köteles válaszolni, illetve az abban kért vizsgálatot lefolytatni, valamint tájékoztatást megadni. Ennek elmaradása esetén a megkeresett hatóság sürgős esetben ideiglenes intézkedést fogadhat el a saját területén, végső esetben pedig a Testület elé kerülhet az ügy, a hatóságok közös döntést hoznak benne.

Közös műveletek

A közös művelet egy egészen újszerű eljárásrend a GDPR-ban, aminek lényege, hogy több hatóság munkatársa vesz részt egy konkrét eljárás végrehajtásában. Ennek részeként akár arra is sor kerülhet, hogy egy másik tagállam munkatársa vizsgálati hatáskört gyakorol az adott tagállamban. Ez az egyik legerősebb együttműködési forma, várhatóan óvatosan fognak ezzel élni a hatóságok, mert sok eljárásjogi kérdés merül fel, és maga a GDPR is több feltételt támaszt annak gyakorolhatóságával szemben.

Az Európai Adatvédelmi Testület

A GDPR által hatályon kívül helyezett 95/46/EK számú adatvédelmi irányelv által korábban létrehozott ún. 29-es Munkacsoportot felváltó Testület szintén jelentős intézményi változás. Önmagában az is nagy újdonság, hogy a Testület jogi személyiséggel rendelkező uniós szervként van definiálva. Erre azért van szükség, mert önálló döntéseket hoz. Nem csak tanácsadó szerv már, amilyen a 29-es Munkacsoport volt, hanem döntései kötelező erejűek, azokból jogok és kötelezettségek fakadnak. A testületi döntések közvetlenül nem az adatkezelőket vagy az érintetteket kötelezik, illetve ruházzák fel jogokkal, csupán közvetett módon kerül erre sor. A Testület döntését a tagállami hatóság által meghozott döntés fogja végső soron érvényesíteni.

A Testület véleményei

A GDPR 64. cikke szerint a tagállami adatvédelmi hatóság ki kell, hogy kérje a Testület véleményét, mielőtt bizonyos döntéseket elfogad. Ide tartozik például az adatvédelmi hatásvizsgálati lista összeállítása. Ezek a listák határozzák meg azokat az adatkezeléseket, amelyek a

magánszférára gyakorolt kockázatok okán előzetes adatvédelmi hatásvizsgálatot igényelnek. A hatásvizsgálati listán túl tipikusan az önszabályozás és a harmadik országba irányuló adattovábbítás témaköreiben kell még kikérni a Testület véleményét. A Testület véleménye a tagállamra nézve tulajdonképpen kötelező, hiszen ha az adatvédelmi hatóság nem követi az abban írtakat, akkor vitarendezési eljárásra kerül sor. Erős eszköz tehát a Testület számára a vélemény kibocsátása a GDPR egységes és következetes jogalkalmazásában.

A Testület vitarendező funkciója

Ha a tagállamok határon átnyúló adatkezeléseket érintő bizonyos kérdésekben nem tudnak megállapodni, akkor a Testület hoz kötelező döntést. Ilyen eset lehet, ha negatív vagy pozitív hatásköri összeütközés merül fel a hatóságok között, vagy az egyablakos ügyintézés során nem jutnak megállapodásra. Szintén vitarendezést igényel az a helyzet, amikor a Testület véleményét nem követi valamely tagállam hatósága. Az első körben kétharmados, második körben már csupán többségi testületi szavazás során minden tagállamnak egy szavazati joga van, súlyozás nélkül.

Sürgősségi eljárások

A GDPR egyik, ez idő szerint nyitott kérdése, hogy mikor és milyen helyzetekben élnek majd a hatóságok a sürgősségi eljárás nyújtotta lehetőséggel. A kulcsszó itt az érintettek jogainak és érdekeinek védelme. Ebből a célból lehet fellépni, akár úgy, hogy egy tagállam a sürgető helyzetre való tekintettel, be nem várva az együttműködési eljárások végét, a saját területén ideiglenes intézkedést fogad el. A másik lehetőség, hogy egy tagállam kéri annak megállapítását, hogy sürgős szükség áll fenn egy adott tagállamban. Ilyen esetekben a Testület véleményt

is kiadhat, de akár kötelező erejű döntést is hozhat. Figyelemre méltó, hogy az adatvédelmi hatóságok közössége kollektív módon lép fel.

Ha nagyon ki akarjuk hegyezni az állítást, akkor azt mondhatjuk, hogy az Európai Uniónak egy nagy adatvédelmi hatósága jött létre a Testület megalakulásával. Egy jogszabály, egy hatóság, teljes harmonizáció – ebben foglalható össze a jogalkotói szándék. Ami a harmonizációt illeti, nem a GDPR újítása, már az 1995-ös adatvédelmi irányelv is a teljes harmonizációt tűzte ki célul, és ezt az Európai Unió Bírósága a legelső elé kerülő adatvédelmi ügyben, a *Lindqvist*[2] ítéletben is megerősítette. Ezen a téren a mérce és a cél tehát változatlan, a GDPR azonban a korábbi irányelvhez képest hatékonyabb eszközöket kínál ezen a téren.

A hatóságok egymástól való függősége

Az Európai Unió adatvédelmi jogának évtizedek óta egyik alapelvi jelentőségű szabálya, hogy a tagállami adatvédelmi hatóságok teljes függetlenségben járnak el. Ezen a GDPR sem változtat, ez továbbra is része a szabályozásnak. A gyakorlat azonban ezen jól megjósolható módon változtatni fog.

Az európai adatvédelmi irányelv hatálya alatt nem fordulhatott elő, hogy a tagállami hatóságot olyan álláspont elfogadására kényszeríthették volna, amivel annak vezetése nem értett egyet. A vitarendezési eljárás folytán azonban most már előállhat ez a helyzet. Az is megtörténhet, hogy a vezető hatóság marad kisebbségben véleményével, és neki magának kell azt a határozatot megszövegeznie, amely az általa vitatott álláspontra alapul. A GDPR egységes alkalmazásának ez az egyik intézményes „ára", amit el kell fogadni, és a tagállami hatóságoknak ezeket

2 Európai Bíróság C-101/01. sz. ügy. Bodil Lindqvist 2003 november 6-i előzetes döntéshozatal iránti kérelem, ECLI:EU:C:2003:596

a kereteket tudomásul véve kell a többi hatósággal olajozottan együttműködniük.

A GDPR elfogadtatása az Unión kívüli világgal

A GDPR nem titkoltan világszerte hatást kíván gyakorolni a *privacy* állapotára. Az extraterritoriális hatály azokat a szereplőket is a GDPR szerinti magatartásra kényszeríti, akik egyébként nem telepednek le az Unióban, de tevékenységük mégis hatással van az Unióban tartózkodó személyek magánszférájára.

Azok az országok, amelyek a szabad kereskedelemben érdekeltek, az adatvédelem terén mutatkozó különbségek áthidalását is elképzelhetőnek tartják. A személyes adatok védelme és a szabad kereskedelem szorosan, politikai szinten is összekapcsolódott. 2019 elején az Európai Unió előrehaladott tárgyalásokat folytat Japán adatvédelmi szintjének kölcsönös elismerése érdekében. Bízhatunk abban, hogy a GDPR valóban jelentős globális hatást vált ki, és további államok mutatnak érdeklődést a megfelelő védelmi szintet elismerő bizottsági határozat iránt. Az Európai Bizottság ezekre a tárgyalásokra régóta nyitottságot mutat.

Bírságok és a jogkövetés

A GDPR által radikálisan megemelt bírság összeg nagy hatást gyakorolt az adatkezelők működésére, sokkal magasabb szintre került az adatvédelmi tudatosság. Sajnálatos, hogy ehhez a bírságok összegét ilyen mértékben kellett növelni (az éves világpiaci forgalom 4%-a, illetve húszmillió euró a maximális összeg), de ha a jogkövetés javítása érdekében erre volt szükség, akkor minden bizonnyal helyes lépést tett a jogalkotó.

Azt is látni kell, hogy az online közegben a versenyjogi, fogyasztóvédelmi és adatvédelmi kérdések időnként nagyon közel állnak egymáshoz, átfedésbe is kerülhetnek, ezért nem volt tovább halogatható

az adatvédelmi jogsértések kapcsán a védelem megerősítése és a bírság összegek megemelése. A személyes adatok védelmére vonatkozó szabályozás nem válhatott a védelmi rendszer gyenge láncszemévé.

Zárszó

Az elmúlt években a legnagyobb hatást kiváltó ügyek érintetti joggyakorlásból, illetve egyéni panaszokból indultak ki. Vegyünk két példát alapul:

- A *Google Spain* ügyben[3] egy egyszerű kérelem volt a vita kiindulópontja: egy réges-régen elfelejtett ügyre mutató link még mindig első helyen jelent meg a találati listán, amikor *Costeja* úr nevére rákerestek a Google keresőjében. Ebből az elsőre talán átlagügynek tekinthető vitából fakadt az elmúlt évek egyik legfontosabb bírósági ítélete. Az ítélet nyomán az összes keresőmotor kénytelen volt átalakítani üzletmenetét, és az egyéni panaszok rendezésére külön ügymenetet kialakítani.
- *Maximilian Schrems*[4] a Facebooknál először arról érdeklődött, hogy milyen adatokat tartanak róla nyilván. Az egyszerűnek induló ügy később akkora hullámokat vetett, hogy az EU és az USA közötti megfelelő védelmet biztosító jogi konstrukciót az alapjaitól újra kellett szabályozni. A súlyos hiányosságokat mutató *Safe Harbor* keretrendszert a *Privacy Shield* váltotta fel, amely az első hiányosságait hivatott orvosolni.

Az adatvédelmi jog érvényesülésének fokmérője a folyamatosan az itt és most dimenziójában élő adatalany helyzete. Ha jogai érvényesülését az intézményrendszer el tudja érni, akkor a GDPR és a hatóságok

3 C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] Judgement of the Court ECLI:EU:C:2014:317.

4 C-362/14 Maximillian Schrems v Data Protection Commissioner

működése és együttműködése sikeres. Ha a napi tapasztalat ezzel ellentétes, akkor joggal kérik számon a jogalkotón és a jogalkalmazón, hogy miért nem működik hatékonyan a jogérvényesítés és a jogvédelem.

Minden szereplőnek valamilyen mértékben beleszólása, szerepe és felelőssége van abban, hogy mindez megvalósulhasson, és a GDPR valóban a jogvédelmet fejlesztő, jogvédelmet erősítő normaként vonuljon be a jogtörténetbe.

Dr. Norbert Csizmadia[5]

The Application of GDPR by Corporations – Experiences and Challenges[6]

Establishing GDPR-compliant practices required significant efforts from companies which are controllers or processors of personal data. These efforts included, inter alia, adoption of new processes, tools, adjusting IT-systems, organizing interdisciplinary work and cooperation, training employees and raising awareness amongst their clients.

Large enterprises were in a better position to tackle these challenges, as they could allocate the necessary resources to their compliance projects. The participants agreed that the preparations required significant investments, and even with having the necessary resources at hand, the two-year long transition period proved to be too short (e.g. software vendors realized their solutions are not able to provide a delete function, development took a significant amount of time). Companies chose different approaches to reach their aims – in certain cases the process is managed by their corporate headquarters, in other cases the local subsidiaries are trusted to run their own compliance program.

However, GDPR is not only applicable to multi-national enterprises. Small companies or self-employed entrepreneurs face similar challenges, but they are not able to employ legal or data protection professionals. The participants of the discussion – with the active participation of the members of the audience – tried to find the answer

5 Corporate Counsel, National Instruments

6 Summary of the Roundtable Discussion with the Members of the AmCham (American-Hungarian Chamber of Commerce) Regulatory Committee representing major corporations on the Hungarian market.

whether following a reasonable approach, proportionate with the size, nature and risk profile of the given data processing would help to mitigate the risks associated with a potential non-compliance – it is at least questionable whether the state authorities will find the "reasonable" approach satisfactory.

The panelists highlighted that the data protection authority could take on a greater involvement in providing individuals with more detailed guidance to foster the effective exercise of their rights granted by the GDPR, and in providing more detailed guidance to small and medium-sized enterprises, to assist their compliance efforts. National legislation should also speed up the process of adjusting sectorial laws with the GDPR, filling the legislative gaps and eliminating parallel regulations.

Is the so-called "GDPR-panic" over? Definitely not. Understanding the GDPR requires a mindset change. Data controllers and data subjects need to understand concepts like pseudonymization of data or privacy by design; common people need to learn what consent or legitimate interest is, and how they can exercise their rights granted by the Regulation.

Two questions remain unanswered, though.

1. Are national data protection authorities now ready to oversee commercial companies' compliance with the legislation, protecting the individuals' rights?

2. Will these authorities provide the same level of protection for the individuals vis-á-vis state offices?

Összegzés

Conclusions

Gizem Gültekin-Várkonyi[1]

Life after the GDPR: Dreaming of a Uniform Application

Like the oil-rich countries, the data-rich countries or companies, even individuals who invest in technologies that could collect and manage data are the most powerful today, and they certainly will be in the future. If we look at some of the largest and most valuable companies in the world[2], we will easily realize that first they are either American or Chinese tech companies, and then they are the ones who have sufficient tools and technologies to collect and manage data. Their continuous investment in such tools as Artificial Intelligence has been a real game changer for them. Examples of such companies could be Facebook, Alibaba, Amazon or Google.

People voluntarily and freely contribute to the world of personal data through their social media accounts, web browser, the transactions they make electronically shopping online. They leave their digital fingerprints in every corner of the virtual world where it does not matter who they are but what data they are represented by. They post wherever they are, whatever they eat, their taste in movies, political views, health-related issues, or they even post their pictures showing all biometric features, videos disclosing their voice, and so on.

As a result of such constant contributions, all that needs to be done by action-ready entities is to analyze that data to offer more personalized

1 Information Management BA and International Relations MA. PhD student, University of Szeged, Faculty of Law and Political Sciences.

2 https://www.forbes.com/powerful-brands/list/#tab:rank Last accessed: 16 December 2018

services fitting people's preferences the most. Be it companies or governments, these entities have already realized the power of the data to predict, to profile, and to manage people's behavior. The most interesting in this story is that people do not really know about the existence of these practices or about the consequences of this fact, the fact that is called "datafication"[3].

What might be the consequences of such datafication? Certainly, people would like to enhance their life by receiving personalized healthcare services which must be uniquely offered in accordance with their own health status. People surely would like to get tips for their financial arrangements or would like to express their political opinions, because we are still humans, and we live in environments where we communicate with humans.

Freedom of speech, freedom of thought, our right to access to medical assistance and many such fundamental principles are basic values of our democratic societies. However, unfortunately in practice, we are faced with some issues that affect our life to the core, and I must stress that there are issues that we are not yet aware of. Some, of course, we are already aware of like the Snowden revelations or the Facebook-Cambridge Analytica scandal (the Wylie revelations, as we prefer) but these only prove how far surveillance could extend through manipulating people's political choices, collecting and transferring their data somewhere out of their knowledge, or refusing their credit application just because they live in a poor area of the city. All these issues clearly reflect that there are cases in which people are decided about by processing their data outside of the scope of legally specified purposes, and without their knowledge, in a way that could do harm to both the individual and the society.

To battle all of these still dangerous trends and issues, data protection was one of the fundamental rights that was first recognized in

3 Mayer Schönberger, V., Cukier, K. (2013), Big data: A revolution that will transform how we live, work and think. London: John Murray.

Europe in the 1970s. Sweden was the first country adopting a national law on protecting personal data in 1973. Council of Europe's Convention 108[4] (on the protection of personal data against computerized processing of personal data) was signed and ratified in 1981 by most of its Members, and today, its scope has become wider since countries such as Argentina, Mexico, Tunisia, Senegal also signed it. These countries voluntarily choose European data protection rules for their citizens although they are far from Europe geographically. Although most of the EU Member States already adopted data protection rules similar to the Swedish Data Protection Act and/or Convention 108, the adoption of the Directive 95/46/EC[5] (as an "updated version" of Convention 108), created the basis for the European Union way of data protection. Strong data protection rules have been developed since then and today, Europe and the EU is in such a position where its legislation has been taken as a guidance not only by most of the European countries, but also globally.

The EU especially tried to construct one of the strongest data protection laws in the world. However, there is still a need for balanced protection, especially in light of such well-referred exceptions as national security, where the EU sometimes lifts its own legal instruments whenever a controversy between the right to data protection and some compelling Member State objectives arise.[6] The invalidation of the so-called Data Retention Directive in 2014 could be one of the most significant

4 ETS No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981. Convention 108 has been updated on 18 May 2018. The updated text reveals many similarities with the GDPR such as, requirements for obtaining consent, right to not to be subject to a purely automated decision, references to the Data Protection by Design rules, etc.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

6 Ojanen, T. (2014). Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, 10 EuConst 528.

examples to this. In that case, the Court of Justice of the European Union did not fear to decide in favor of data protection rights of individuals even if it amounted to invalidating an agreement between the EU and the US, two strategic, political, and trade partners. As it is referred in many papers within this book, the Schrems case invalidating the Safe Harbor agreement between the EU and the US enabling legal flows of personal data between the two, could be another example.

All these issues caught the EU lawmakers' attention and they decided to comprehensively update EU data protection rules. Since the GDPR was drafted in 2016 and entered into force on 25 May 2018 they are "market leaders" in this field. Targeting uniform application in all twenty-seven Member States is a commendable vision but since every Member State has its own approach to interpret the privileges of the GDPR, it might prove harder than it seems. In this paper, we would like to shortly highlight some of the novelties of the GDPR, then introduce the meaning of the Regulation in the EU legal sphere. Finally, I will discuss the chances of the uniform application of the Regulation by using Sweden as an example. The Swedish case is particularly worth examining further because of the country's well-known American-type liberal approach to data-based market and economy which is, if not fully, contradictory to the EU's rights-based approach. In the view of such an approach, we could easily realize how the GDPR could be circumvented by some Member States interpreting the exemptions in a broad sense.

The Nature of Regulations in the EU and the Novelties of the GDPR

First of all, better protection for individuals by broadening interpretation of already existing principles and the introduction of new rights for them to tackle the problems raised by technological developments are certainly key novelties of the Regulation. The right to be forgotten

or right to erasure, strengthened consent rules and the right to request a copy of personal data processed are just some further examples of the improvements brought about by the GDPR. All of these stronger rights for data subjects and the obligations imposed on data controllers could be called as "GDPR direct effects on individuals", which also shape the specific legal nature of the Regulation as part of the EU legal order.

The EU is a unique supranational entity both from the aspect of its construction and its procedures. One of the reasons for its uniqueness admittedly is its legal construction and its effects on the Member States. The EU operates based on the founding treaties, which provide the general framework of its scope of action and where the Member States are bound to implement and apply EU legal acts.

The founding treaties and their amendments are the primary sources of EU law. Secondary sources consist of several other legal instruments based on the founding treaties and on the top of their hierarchy, regulations are those legal acts that are directly applicable, i.e. they do not have to be transposed into national law, but enforced as national law.

Article 288 of the TFEU confirmed former Article 189 of the EEC indicating and states that *"[a] regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States*." In interpreting the treaties, the CJEU created a case law, based on which where MS failed to apply regulations it was said that Member States do not have a room for maneuver to apply them partially or apply as they wish. In a preliminary ruling case referred on 14 December 1971 by *Politi s.a.s. v Ministry for Finance of the Italian Republic*, the *Tribunale civile e penale di Torino* referred a question to the Court of Justice whether particular articles in Regulation no 121/67/EEC of the Council of 13 June 1967 on the Common Organization of the Market in Pigmeat[7] *"are immediately applicable within the national legal system*

7 Regulation No 121/67/EEC of the Council of 13 June 1967 on the common organisation of the market in pigmeat

and, as such, create individual rights which national courts must protect".[8] The Court answered by referring to the Article 189 of the EEC and indicated that *"by reason of their nature and their function in the system of the sources of Community Law, Regulations have direct effect and are as such, capable of creating individual rights which national courts must protect. Court further referred to the effect of a Regulation which "prevents the implementation of any legislative measure, even if it is enacted subsequently, which is incompatible with its provisions"*. In another case, *Commission of the European Communities v Italian Republic*, the Court of Justice drew the attention of the Italian authorities to the fact that a Member State cannot opt out of Regulation provisions and Regulations are effective from the date they were published in the Official Journal[9]. This is a particularly important case since it highlights that obedience to regulations is important from the date of their publication[10].

Prior to the GDPR, the EU's data protection legislation was guided by a "softer form" of an EU legal act, Directive 95/46/EC. Unlike Regulations, Directives are "softer" due to their importance in securing the uniformity of the EU law, giving a certain margin of appreciation to the Member States to implement the regulatory objectives specified by the Directive. Its initial purpose is harmonization of EU law, not unification, being the ultimate aim of Regulations. Article 288 of the TFEU states that *"[a] directive shall be binding, as to the result to be achieved,*

8 61971CJ0043, Judgment of the Court of 14 December 1971. - Politi s.a.s. v Ministry for Finance of the Italian Republic, ECLI:EU:C:1971:122

9 61972J0039 Judgment of the Court, 7 February 1973. - Commission of the European Communities v Italian Republic. Premiums for slaughtering cows. - Case 39-72.

10 Indeed, the Commission could monitor the Regulation's application status in case the Member State is fully ready to implement, but first, the Commission needs a well-founded suspicion before referring the case to the Court. Finally, we think that it is practically impossible to check every Member State on a daily basis whenever a Regulation or any other legal instrument is adopted.

upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods"[11].

This distinction is very important in the legal force of data protection rules as well. Practically, under a directive, we would find 28 different ways of implementation, but topics subject to a Regulation are applied "as is". Regulations are strong legal acts and increasing the force of privacy protections and personal data protection was undoubtedly one of the reasons why Directive 95 was switched to a Regulation. It was important to take this step, especially since China and US data protection challenges the EU's approach from several points.

Before the GDPR, some Member States had stricter data protection rules than others. Traditionally, Germany and Austria are known of their stricter data protection regimes than those of Ireland, Italy and Romania. Indeed, it is not a surprise that the European headquarters of some of the tech giants (Facebook, Google) were all settled in Ireland. Most of the Member States were not taking the right to data protection into account in their political discussions, awareness regarding data protection issues was low.[12]

Hoping the GDPR would open a new blank page in the European way of unifying data protection rules, I still think that a completely uniform application of the GDPR practically will not be possible, at least in the near future.

Switching from a Directive with twenty-three years of practice (with low general awareness standards) to a Regulation in two years' time is not an easy task for the Member States. In the practices that developed in implementing Directive 95/46/EC exceptions and solutions unique to the Member States have been created, and now a global change of mindset is required. I would like to illustrate this with the Swedish example.

11 Becker 1982 Tobler C., Beglinger, J. Essential EU Law in Text, Lap- és Könyv Kiadó, Budapest, 2010. p.43 Van Duyn case; Judgment of the Court of 4 December 1974. Yvonne van Duyn v Home Office. ECLI:EU:C:1974:133.

12 Custers, B., Dechesne, F., Sears, A.M., Tani, T., van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU, Computer Law & Security Review 34, 234–243.

The Origins of Data Protection Law in Sweden and the Swedish Path to the GDPR

Sweden is the first country in the world that adopted a national personal data protection law, the Data Protection Act, in 1973.[13] There were huge differences between today's data protection legislation and the laws of that time. Today's technology is completely different than the technology in the 70s. Computerized processing of personal data only became an issue underlying Convention 108 (as we have seen above) in the 1980s. In the Sweden of the 1970s, data could be processed only if the Swedish Data Protection Board (*Datainspektionen*) would give permission to the data controller[14]. The Swedish Data Protection Act was updated from time to time with minor changes, but a comprehensive revision occurred when Sweden became an EU member in 1995. Until the adoption of the GDPR the amendments continued, but it certainly has brought the biggest change in Swedish data protection legislation.

The Swedish Data Protection Act – although the oldest – was very general in its scope which was made whole through sector-specific legislation on data processing. As a result, there were different data protection laws in different fields such as healthcare,[15] crediting,[16] electronic

13 Technically, historical record shows that the German Land of Hessen has indeed put in place a „national" data protection law in 1970, but due to the federal structure of the German State it is not considered hereby as a „national data protection law". The German federal Datenschutzgesetz (which now qualifies as a Member State regulation) was finally adopted, based on the Hessen example in 1978, thereby became only the second „national data protection law" to be adopted for the purposes of the above historical description.

14 Öman, S. (2004) . Implementing Data Protection in Law, in IT Law, Wahlgren, P. ed., Scandinavian Studies in Law, The Stockholm University Law Faculty, 47, pp.390-403, p400.

15 Patientdatalagen (2008:355) (Patient's Data Act).

16 Kreditupplysningslag (1973:1173) (Credit Information Act).

communications,[17] camera surveillance[18] and so on, making up a "complex system".[19]

Although Sweden was the first to have legal protection for data protection rights of individuals, its approach to the subject was criticized several times. A report published by the Human Rights Committee comprising representatives from Privacy International, Civil Rights Defenders and DFRI (*Digital Freedom and Rights Association or Föreningen för Digitala Frioch Rättigheter*)[20] states that the Swedish Act on Signals Intelligence in Defence Intelligence Operations[21] gives power to the Swedish National Defense Radio Establishment to collect data from transnational communications through analyzing search terms of groups of people from different nationalities. However, practice shows that only a small percentage of collected data is relevant to the targeted aim (national defense). Furthermore, it was reported that the Act was unclear on the parties that were legally authorized to collect data, and both the State Inspection for Defence Intelligence (i.e. the oversight mechanism for intelligence-related data protection) and the Defence Intelligence Court which authorizes data collection for intelligence, were found lacking independence and transparency. This example is important to understand how legal exemptions could sometimes cause conflicts.

The following example presents how some of the Swedish actors in the data protection field may mistakenly interpret the essence of the regulation which may cause the misapplication of the GDPR. In a report discussing protection of personal health related data, it was referred that health data is being collected and stored in medical devices

17 Lag (2003:389) om elektronisk kommunikation (Electronic Communications Act)
18 Kameraövervakningslag (2013:460) (Camera Surveillance Act)
19 Öman, p.400.
20 https://privacyinternational.org/sites/default/files/2017-12/HRC_Sweden_0.pdf Last accessed 25 November 2018
21 Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet

in Sweden by the Swedish Management Network for Biomedical Engineering[22] within the framework of the Swedish Patient Data Act, the Patient Safety Act and the Medical Devices Act. However, since these acts did not use a uniform definition of "medical device data" which is almost any data about a patient collected by devices, Swedish people's data protection right was not fully protected.

Also, the above-mentioned Acts had different approaches and sometimes very narrowly tailored (legal and other security) measures to protect such data. As a result, besides security- and technology-related recommendations, the Swedish Management Network for Biomedical Engineering proposes to harmonize the examined Acts with EU personal data protection legislation. As indicated in the report, *Datainspektionen* was the only opposing party to this statement, and I think that it is most probably because the wording "harmonization" was used instead of uniform application.

Now I will try to explain how the GDPR may be a challenge for Swedish courts regarding to the country's traditions of a differently balanced data protection culture.

The Swedish Data Protection Act was updated based upon the GDPR and the new legal text was prepared on 19 April 2018, and following adoption, it entered into force on 25 May 2018. Sweden is one of the countries that did not miss the GDPR's *de jure* enforcement deadline. In her article, Jonason (2018)[23] comprehensively explains Swedish path to the GDPR. About two months after the GDPR was officially announced

22 The Swedish Management Network for Biomedical Engineering, The Swedish Patient Data Act in the clinical everyday- What demands are made on medical devices? Condensed Report Part 2: Application of information security in medical devices and systems 30 September 2016 English version 23 October 2017 http://www.lfmt.se/Filer/SI-forum/uppladdade%20dokument/LfMT%20-%20The%20Swedish%20Patient%20Data%20Act%20in%20the%20clinical%20everyday%20-%20Condensed%20Report%20Part%202%20-%20171023.pdf

23 Jonason, P. (2018). The Swedish Measures Accompanying the GDPR, in Mc Cullagh K., Tambou O., Bourton S. (Eds.), National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxembourg February 2019, 130 pages. Available at: https://wp.me/p6OBGR-3dPp.6.

in the EU's Official Journal, two groups were assigned by the Swedish Government to prepare Swedish legislation for GDPR: Data Protection Inquiry (DPI) for preparing the legal provisions and a Data Protection Committee (DPC) for discussing the questions related only to institutional construction. DPI comprehensively examined the GDPR and drafted the first version of the new Act in May 2017. After the ordinary consultations and revisions, the Swedish Parliament adopted the new Data Protection Act. Jonason[24] notes an important point from the DPI's report that they did not have enough time to examine all the aspects in a deeper manner which may have amounted to better differentiations in the Act.

Jonason's further analysis points to Sweden's unique approach to the GDPR in cases where the right to data protection and freedom of expression need to be balanced.[25] Processing of personal data based on solely journalistic purposes which was an exemption under Article 9 of Directive 95/45/EC, which still is under GDPR Article 85, is interpreted in Sweden in the broadest sense. The Swedish Constitutional Court decided in one of its judgments[26] in favor of the petitioner who published some bank employees' personal data on a website to prove malpractices in the Swedish banking system, and stated that this act was based on a journalistic purpose, i.e. to inform the public. The Swedish Supreme Court (Högsta domstolen) interpreted the case based on the ECHR and the case law of the ECtHR. Although *Datainspektionen* criticizes the Court's decision, no further steps were taken.

From the point of view of the Court of Justice, Sweden's data protection approach that is more expression- and press-centric may not be acceptable. In *Dennekamp v European Parliament* where Dennekamp (a Dutch journalist) asked for MEPs' pension scheme documents, the

24 Ibid., p.43

25 The first Freedom of Press Act dates back to 1776 in Sweden.

26 Case B 293-00, judgment of 12 June 2001, Referred from, Bygrave, L. (2002). Data Protection Law —Sweden: Balancing Data Protection and Freedom of Expression in the Context of Website Publishing — Recent Swedish Case Law, Computer Law & Security Report, 18 (1).

CJEU rejected any claims to providing the documents stating that the MEP's personal data cannot be transferred without a clear expression of necessity. Based on the very clear logic of the existence of public interest information, the applicant claimed that those documents are important *"for European citizens to know which MEPs had a personal interest in the additional pension scheme when called upon to take decisions regarding its management"*[27], and accessing personal data in the documents is necessary in line with the right to information and the right to freedom of expression which could serve for European citizens to see *"how public money was being spent, on the possible impact of private interests on the voting behavior of the MEPs and on the functioning of control mechanisms"*, but the Court still did not annul the decision of the EP which found applicant's statements unconvincing in their examination of necessity.

Finland, EDPS, and as expected, Sweden (intervening) were in favor of the applicant, reporting that the documents could serve transparency of the EP and MEPs. The case shows how the CJEU and Sweden reflect divergent positions about interpreting the right to information and the right to freedom of expression, and transparency of public institutions.

Obviously, the Swedish legislator updated the Data Protection Act in a way that the GDPR still cannot precede the Freedom of the Press Act and the Fundamental Law on Freedom of Expression. Although Swedish *Datainspektionen* warned the Swedish Government (*Regeringskansliet*) about the fact that Regulation is one of the legal instruments of the EU which shall be directly implemented, it was not taken into consideration. However, and evidently, Swedish lawmakers were already aware of this situation since an explanation was delivered regarding the judgment stating that *"previous provision of the Personal Data Act with a similar content had not been the subject of legal challenges nor*

27 Case T-115/13, Judgment of the Court of 15 July 2015, Gert-Jan Dennekamp EU:T:2015:497

had it been questioned by the European Commission during its 20 years of application"[28].

If these statements remain same for the next couple of years, and if Sweden will not be referred to the CJEU for breach of EU law by the Commission, then we should not even wait for robots to come alive to question the uniform application of GDPR in practice. Some countries like Sweden already interpret the Regulation in their own way.

Another example could help to illustrate the situation further[29]. In Sweden, the owner of a publicly available database may get a publisher's license which then will enable them to protect and control the content they publish. With this license, they can import personal data such as phone numbers without consent. Since Swedish law puts the GDPR in a weaker position in case of a conflict with freedom of expression, database owners take this opportunity to build their own databases full of personal data collected without data subjects' knowledge.

One more point in the assessment of the above-cited Jonason shows how the Swedish point of view of the GDPR is different from the spirit of the law itself. As she argues, the Swedish legislator shaped the Data Protection Act in such a way that it is not "abuse-centric" but opts for a "regulatory model" which means that some of the data breaches may be tried to be repaired through retrospective inspection. Government's notification taking into account that deciding on the violation should "not [be] based on the release itself but after the release" is evident[30], pointing its opinion as a later on response to the breaches of rights of data subjects. However, once data is made available out of data subject's consent or knowledge, even though it happens accidentally, it is almost impossible to take an ex post action to remove the negative effects. Such

28 Jonason, p.6.

29 Meyer, D., Sweden's open society is clashing with EU privacy law, and regulators are frustrated, 22 May 2018, IAPP. Available: https://iapp.org/news/a/swedens-open-society-is-clashing-with-eu-privacy-law-and-regulators-are-frustrated/

30 Swedish Government Official Report SOU 2017:52. Referred from, Storr, C., Storr, P. (2018). Sweden: Quantitative (but Qualitative) Changes in Privacy Legislation, 4 Eur. Data Prot. L. Rev. 97

statement also goes against the much-desired logic of Data Protection by Design which requires proactive or ex ante action rather than retrospective measures in protecting privacy.

Storr and Storr[31] refer to the previous Swedish Data Protection Act and argue that it seems stricter than the updated one since the Swedish legislator (*Riksdag*) chose to apply loosened rules of consent, data minimization and purpose limitation for personal data[32]. Finally, the Swedish legislator's opposition to *Datainspektionen* contains some messages reflecting on the future Swedish application of the GDPR. For example, when *Datainspektionen* raised its voice several times on several topics, from lowering the age limit for a child's consent from fifteen to thirteen[33], and warned the lawmaker regarding the way they try to interpret the GDPR, it was not taken seriously by the legislator.[34] This approach shows how authority of a National Supervisory Authority whose competences increased in the GDPR could be shaken even more drastically in the future.

Based on the above statements, Sweden had some problems with interpreting Directive 95/46/EC, and has some obstacles with understanding the GDPR, and finally, the sector-based practices where the Swedish Data Protection Act was excluded could sufficiently and comprehensively cover the issues.

31 Ibid., p102.

32 Ibid. 97. Authors call such data processing "unstructured" which is a term derivable from Article 4 (6) of the GDPR giving the definition of 'filing system': *"any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."* It seems that the Swedish legislator thought that if there was a structured set of data, then there must be unstructured data too, so such data should be exempted from the scope of the GDPR.

33 Ibid. p,100

34 Jonason, p.7

Conclusion

The GDPR is the most up-to-date legal document on data protection introducing new rights for data subjects, as well as introducing new rules and obligations to data controllers. Member States of the European Union have a duty to ensure GDPR's full application, but first, they must adopt it in accordance with the spirit of the Regulation.

Unlike Directive 95/46/EC, the GDPR does not leave room for so many different interpretations and implementations. As the Swedish example reflected above, Member States' specific traditions and implementations hedge off the demanded uniform application of the GDPR, although it offers **Good Data Protection Rules** for the data controllers and **Good Data Protection Rights** for EU citizens.

Irodalomjegyzék/Bibliography

Ügyek / Cases

1. C-101/01. sz. ügy. Bodil Lindqvist. 2003. november 6-i előzetes döntéshozatal iránti kérelem, ECLI:EU:C:2003:596
2. C-T-115/13, Judgment of the Court of 15 July 2015, Gert-Jan Dennekamp EU:T:2015:497.
3. C-131/12. sz. ügy. Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González. A bíróság 2014. május 13-án kelt ítéletе ECLI:EU:C:2014:317.C-311/18. sz. ügy. Facebook Ireland és Schrems. 2018. május 9-én kelt előzetes döntéshozatali kérelem, folyamatban lévő ügy.
4. C-362/14 sz. ügy. Maximillian Schrems és a Data Protection Commissioner. A bíróság 2015. október 6-án kelt ítéletе, ECLI:EU:C:2015:650).
5. Commission of the European Communities v Italian Republic. Premiums for slaughtering cows. - Case 39-72. Judgment of the Court, 7 February 1973.
6. Politi s.a.s. v Ministry for Finance of the Italian Republic, Judgment of the Court of 14 December 1971. ECLI:EU:C:1971:122.

Jogalkotás / Legislation

1. A Kormány tagjainak feladat- és hatásköréről szóló 94/2018 (V.22.) Korm. Rendelet.
2. A Polgári Törvénykönyvről szóló 2013. évi V. Törvény.

3. A személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv (Irányelv).
4. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.).
5. A személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet).
6. Az Európai Unió Működéséről szóló Szerződés (egysége szerkezetbe foglalt változat).
7. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról szóló 2018. évi XXXVIII. törvényhez fűzött indokolás, http://www.parlament.hu/irom41/00623/00623.pdf
8. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról szóló 2018. évi XIII. törvényhez fűzött indokolás, http://www.parlament.hu/irom41/00335/00335.pdf
9. Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)
10. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

11. ETS No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981.
12. Magyarország Alaptörvénye (2011. április 25.).
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
14. Regulation No 121/67/EEC of the Council of 13 June 1967 on the common organisation of the market in pigmeat.
15. 15/1991. (IV.13.) AB határozat.
16. 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

Tudományos cikkek / Academic Resources

1. Voigt, P., von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer International Publishing AG, Switzerland.
2. Ojanen, T. (2014). Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, 10 EuConst 528.
3. Custers, B., Dechesne, F., Sears, A. M., Tani, T., van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU, Computer Law & Security Review 34, 234–243.

4. Öman, S. (2004). Implementing Data Protection in Law, in IT Law, Wahlgren, P. (ed.), Scandinavian Studies in Law, The Stockholm University Law Faculty, 47, pp.390-403
5. Bygrave, L. (2002). Data Protection Law — Sweden: Balancing Data Protection and Freedom of Expression in the Context of Website Publishing — Recent Swedish Case Law, Computer Law & Security Report, 18 (1).
6. Jonason, P. (2018). The Swedish Measures Accompanying the GDPR, in Mc Cullagh K., Tambou O., Bourton S. (Eds.), National Adaptations of the GDPR, Collection Open Access Book, Blog *droiteuropeen*, Luxembourg February 2019, 130 pages. Available at: https://wp.me/p6OBGR-3dP
7. Storr, C., Storr, P. (2018). Sweden: Quantitative (but Qualitative) Changes in Privacy Legislation, 4 Eur. Data Prot. L. Rev. 97
8. Mayer Schönberger, V., Cukier, K. (2013), Big data: A revolution that will transform how we live, work and think. London: John Murray.
9. Meyer, D., Sweden's open society is clashing with EU privacy law, and regulators are frustrated, 22 May 2018, IAPP. Available: https://iapp.org/news/a/swedens-open-society-is-clashing-with-eu-privacy-law-and-regulators-are-frustrated/
10. Reinsel, D., Gantz, J., Rydning, J. Data Age 2025: The Digitization of the World From Edge to Core, November 2018, IDC. Available: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Internetes hivatkozások / Internet Resources

1. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en
2. https://www.forbes.com/powerful-brands/list/#tab:rank

3. https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/
4. https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf
5. https://privacyinternational.org/sites/default/files/2017-12/HRC_Sweden_0.pdf
6. http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm

Vegyes / Miscellaneous

The Swedish Management Network for Biomedical Engineering. The Swedish Patient Data Act in the clinical everyday – What demands are made on medical devices? Condensed Report Part 2: Application of information security in medical devices and systems 30 September 2016 English version 23 October 2017

Az Európai Unió társfinanszírozásával

ISBN 978-963-306-270-8
ISSN 2064-4639