Akkreditáció és tanúsítás, magatartási kódexek, harmadik országba történő adattovábbítás

Dr. Szabó Endre Győző – Dr. Majsa Ágnes Judit

NEMZETI KÖZSZOLGÁLATI EGYETEM
BUDAPEST

Szerzők:
Dr. Szabó Endre Győző
Dr. Majsa Ágnes Judit

Szakmai lektor:
Dr. Péterfalvi Attila

A kézirat lezárásának dátuma:
2019. november 22.

Kiadás éve:
2020

TARTALOM

1. BEVEZETŐ

A GDPR 7. tantárgyhoz kapcsolódó tananyag először a személyes adatok harmadik országba történő továbbítására vonatkozó feltételrendszert mutatja be, majd a magatartási kódexekre és végül a tanúsításra és az ahhoz kapcsolódó akkreditációra vonatkozó, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendeletben (a továbbiakban: általános adatvédelmi rendelet vagy GDPR) lefektetett szabályokat. Ennek oka, hogy az V. fejezetben található, a személyes adatok harmadik országba történő adattovábbítására vonatkozó kötelezettségek, rendelkezések – bár elkülönült fejezetben szerepelnek a jogszabályban – az adatkezelők és adatfeldolgozók általános, minden esetben alkalmazandó kötelezettségei. Az itt részletezett követelményeknek ugyanis minden esetben meg kell felelni, amennyiben az Európai Gazdasági Térségen (a továbbiakban: EGT) kívüli adattovábbítást kíván végrehajtani egy adatkezelő vagy adatfeldolgozó.

Ezzel szemben a tanúsítás, illetve a magatartási kódex olyan, a GDPR által létrehozott eszközök, amelyeket az adatkezelők és adatfeldolgozók önkéntesen alkalmazhatnak, és amelyeket felhasználhatnak az általános adatvédelmi rendeletben előírt követelményeknek való megfelelés igazolása során. A két eszköz ezáltal számos hasonlóságot mutat, amelyeket a tananyag vonatkozó részeiben is kifejtünk csakúgy, mint az egyes eszközök sajátosságait és részletszabályait.

A GDPR által bevezetett elszámoltathatóság alapelve megköveteli az adatkezelőtől, hogy igazolni tudja az ebben foglaltaknak való megfelelést. Ennek számos eszköze lehet, melyeknek egy részét a GDPR is nevesíti. A GDPR által nevesített eszközök közül vannak, amelyek meghatározott esetekben kötelezően alkalmazandók (például az adatkezelési tevékenységek nyilvántartása, adatvédelmi incidens bejelentése a felügyeleti hatóságnak, adatvédelmi hatásvizsgálat). A GDPR azonban olyan eszközöket is megnevez, amelyeknek alkalmazását nem teszi az adatkezelő kötelezettségévé, vagyis önkéntesek. Mind a magatartási kódex, mind a tanúsítás ilyen önkéntes eszköz, amelyet az adatkezelő vagy adatfeldolgozó felhasználhat annak bizonyítása során, hogy megfelel a GDPR előírásainak. Közös előnye lehet ezeknek az eszközöknek, hogy önkéntességük okán az érintettekben bizalmat ébreszt az ezeket alkalmazó adatkezelőkkel és adatfeldolgozókkal szemben, hiszen proaktivitást, megfelelésre törekvést mutat a részükről. Emellett elősegíti azt is, hogy adatkezelési tevékenységeik átláthatóbbak legyenek.

2. SZEMÉLYES ADATOK HARMADIK ORSZÁGBA TÖRTÉNŐ TOVÁBBÍTÁSA

2.1. A GDPR elvárásrendszere harmadik országba irányuló adattovábbítás esetén

2.1.1. Bevezetés – a személyes adatok áramlása az Európai Gazdasági Térségen belül[1]

A GDPR a személyes adatok védelmét és a határon átnyúló adattovábbítások esetét minden esetben összeköti. A jogalkotási aktus címe is ezt tükrözi, hiszen tartalmazza egyrészt a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét, továbbá az ilyen adatok szabad áramlásának célkitűzését.

Az Európai Unió azért alkotta meg a személyek magas szintű védelmét szolgáló adatvédelmi normarendszert, hogy aztán az azonos szintű védelem mellett a személyes adatok a közös gazdasági övezetben szabadon áramolhassanak.

Az 1995-ös adatvédelmi irányelv új rendelettel való felváltásának oka többek között abban keresendő, hogy a védelem terén nem sikerült teljes harmonizációt elérni. Az Európai Unió jogalkotója a GDPR (9) preambulum bekezdésében az irányelv végrehajtásával kapcsolatos kritikáját foglalja össze, és itt említi a tagállamonként eltérő védelmi szint problémáját: „[a]z a tény, hogy a személyes adatok kezelése tekintetében a természetes személyek jogai és szabadságai egyes tagállamokban eltérő szintű védelmet élveznek, különösen, ami a személyes adatok védelméhez való jogot illeti, a személyes adatok Unióban történő szabad áramlásának útjában állhat".

A védelmi szintek közötti eltérések kiküszöbölését az Európai Unió rendelet alkotásával látta elérhetőnek, amely jogbiztonságot és áttekinthetőséget ígér. Az azonos szint garantálása kapcsán az uniós jogalkotó néhány aspektust említ, így a jogi úton érvényesíthető jogokat és kötelezettségeket, az adatkezelők és az adatfeldolgozók számára azonos felelősséget, továbbá valamennyi tagállamban azonos szankciók alkalmazását és a tagállami adatvédelmi hatóságok közötti hatékony együttműködést.[2] A védelmi szintek azonossága az adatok szabad áramlása előtt nyitja meg a lehetőséget.

2.1.2. Harmadik országok

A GDPR V. fejezete *A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása* címet viseli. A harmadik ország nem az Európai Unió, hanem az Európai

---

1 A GDPR EGT-vonatkozású szöveg, ennek megfelelően az Európai Unió tagállamain túl alkalmazandó Izland, Liechtenstein és Norvégia vonatkozásában is.

2 A GDPR (13) preambulum bekezdésének első mondata szerint. Ez a jogalkotói célkitűzés már az adatvédelmi irányelvben is fellelhető volt [(8) és (9) preambulum bekezdés].

Gazdasági Térség (EGT) alapján ítélendő meg. Ennek megfelelően az Unió tagállamain túl Izland, Liechtenstein és Norvégia is a GDPR alkalmazási körébe tartozik, tehát annak a térségnek a részét képezik, ahol a személyes adatok áramlásának gátjaként nem lehet hivatkozni a különböző védelmi szintekre. Minden olyan esetben tehát, amikor az EGT-ből irányul nem szerződő fél felé személyes adat, az adattovábbítás a lentiekben megfogalmazott elvárásrendszer alapján ítélendő meg.[3] Az adatok továbbítása terén a köz- és a magánszervezetek adattovábbításai kapcsán adódnak különbségek, ezekre mindenhol ki fogunk térni.

2.2. A személyes adatok védelme harmadik országba irányuló adattovábbítás esetén

A GDPR a harmadik országokat és a harmadik országban működő nemzetközi szervezeteket említi címzettként. Akkor, amikor elemzésünkben harmadik országot említünk, értelemszerűen minden esetben a nemzetközi szervezeteket is értjük e kifejezés alatt.

2.2.1. Az adattovábbítások jogszerűségének két alapfeltétele: a védelem szintje és a jogalap

Amint bemutattuk, az Európai Unión belüli adatáramlás célja többes, egyrészt megfogalmazódik a gazdasági megfontolás, másrészt a tagállami hatóságok hatékony feladatellátása. Ez a kettős célkitűzés a harmadik országba irányuló adattovábbítások szabályozása esetén is érvényesül. Elismeri a jogalkotó, hogy a nemzetközi kereskedelem és a nemzetközi együttműködés bővítéséhez szükség van a személyes adatoknak az Unión kívüli országok viszonylatában megvalósuló forgalmára.[4] Ezek a megfontolások tehát legitimmé teszik az ilyen célú adatforgalmat, és ehhez a rendelet legalitást nyújt. Ennek azonban több feltétele van.

Elvi jelentőségű feltétel, hogy harmadik országba irányuló adattovábbítás esetén „nem sérülhet a természetes személyeknek az Unióban e rendelettel biztosított védelem szintje, és annak fenn kell maradnia az ilyen személyes adatoknak az adott harmadik országból […] történő újbóli továbbítása esetén”.[5] Nem adhat kibúvót az Európai Unió által támasztott elvárásokkal szemben az a körülmény, hogy az adatokat újból exportálják. Amint az Európai Bizottság vonatkozó dokumentumában fogalmaz: a védelem a személyes adatokkal együtt „utazik”.[6]

A másik alapvető és elvi jelentőségű feltétel, hogy a személyes adat továbbításának megfelelő jogalapja biztosított legyen. Abban az esetben, ha az EGT-n belül kerül sor személyes adat továbbítására, akkor is szükség van egy jogalapra az adatkezelés jogszerűségének biztosítása érdekében. Ez a feltétel értelemszerűen érvényesítendő akkor is, amikor a személyes adat továbbítása EGT-n kívüli személy számára történik. Az adatkezelésnek tehát a GDPR 6. cikke alapján jogszerűnek kell lennie.

---

3 Az Egyesült Királyság Európai Unióból való kiválásával harmadik országgá válik.

4 A GDPR (101) preambulum bekezdésének első mondata szerint.

5 A GDPR (101) preambulum bekezdésének harmadik mondata.

6 Az Európai Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A személyes adatok cseréje és védelme a globalizált világban, Brüsszel, 2017. 1. 10. COM(2017) 7 final. A dokumentum angol nyelvű verziója szerint „the protection travels with the data” (2.2. fejezet).

2.2.2. Nemzetközi megállapodások és a GDPR viszonya

Amint bemutattuk, a GDPR általános érvénnyel szabályozza a személyes adatok kezelését, illetve védelmét szerte az Európai Unióban. Ez az általános szabályozási igény a harmadik országba irányuló adattovábbítások esetén is fennáll, mindazonáltal az uniós jogalkotó tiszteletben tartja a tagállamok és harmadik országok között már létrejött, a személyes adatok továbbításáról, illetve az ilyen szerződésekben az érintettek számára nyújtandó megfelelő garanciákról szóló nemzetközi megállapodásokat. A GDPR hatálybalépésekor már érvényes szerződéseket a GDPR tehát nem érinti.[7] A jövőre nézve azonban a GDPR már csak azokat a nemzetközi megállapodásokat nem érinti, amelyek kívül esnek az uniós jog hatályán. Ugyanakkor általános követelményként támasztja minden esetben, hogy biztosítani kell az érintettek alapvető jogainak megfelelő szintű védelmét.[8]

2.3. A megfelelő védelmi szint garantálásának eszközei és ezek rendszere – áttekintés

A GDPR a harmadik országba irányuló adattovábbítás jogi szabályozásának olyan rendszerét hozta létre, amely épít a már több évtizedes gyakorlatra, kodifikálja a hatósági és bírósági jogfejlesztést, továbbá rugalmas elemeket is tartalmaz annak érdekében, hogy a rendszeres felülvizsgálat révén a védelmi szint és a jogbiztonság valóban hosszú távon, a jogi keretek módosítása nélkül szavatolható legyen.

A GDPR első helyen említi, és rendszertani helyét tekintve valóban első helyen áll az úgynevezett megfelelőségi határozat. Az Európai Bizottság megállapíthatja, hogy egy harmadik ország vagy annak valamely területe vagy valamely ágazata, illetve a nemzetközi szervezet megfelelő védelmi szintet biztosít. Ezekben az esetekben a védelem szintjének további igazolására nincs szükség.[9]

Abban az esetben, ha nem áll rendelkezésre megfelelőségi határozat, a GDPR az adattovábbításokat megfelelő garanciák megléte esetén engedi meg. Ezeket a garanciákat az adatkezelőnek vagy az adatfeldolgozónak kell nyújtania, és csak abban az esetben fogadhatók el, ha az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

Megfelelő garanciának minősül
- a közhatalmi vagy közfeladatot ellátó szervek közötti, jogilag kötelező erejű jogi eszköz,
- a kötelező erejű vállalati szabályok, angol kifejezéssel Binding Corporate Rules (BCR),
- az Európai Bizottság által elfogadott általános adatvédelmi kikötések,
- a tagállami adatvédelmi felügyeleti hatóság által elfogadott és az Európai Bizottság által jóváhagyott általános adatvédelmi kikötések,
- a jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó kötelező erejű és kikényszeríthető kötelezettségvállalásaival kiegészítve,
- a tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó kötelező erejű és kikényszeríthető kötelezettségvállalásaival kiegészítve.

A felsorolt hat megfelelő garancia az adatvédelmi felügyeleti hatóság engedélye nélkül garantálja a megfelelő védelmi szintet.[10]

---

7 A GDPR (102) preambulum bekezdésének első mondata szerint.
8 A GDPR (102) preambulum bekezdésének utolsó mondata szerint.
9 A GDPR 45. cikkének (1) bekezdése szerint.
10 A GDPR 46. cikkének (2) bekezdése szerint.

További megfelelő garanciának minősül
- az illetékes felügyeleti hatóság engedélyével az uniós és a harmadik országbeli adatkezelő vagy adatfeldolgozó között létrejött szerződéses rendelkezések, valamint
- szintén az illetékes felügyeleti hatóság engedélyével a közhatalmi vagy közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések.[11]

Az adatvédelmi felügyeleti hatóság engedélyével biztosított megfelelő garanciák esetében ugyan egy-egy tagállami hatóság jár el, azonban ezt a hatáskörüket közösen, az Európai Adatvédelmi Testületben (a továbbiakban: Testület) az ún. egységességi mechanizmus keretében gyakorolják.[12]

A megfelelő védelmi szint garantálásának eszköze lehet még az Európai Unió vagy egy tagállama és egy harmadik ország között létrejött nemzetközi megállapodás.[13]

Az ún. különös helyzetekben biztosított eltérések a megfelelő védelmet nem biztosító országokba való adattovábbításokat teszik szűk körben megengedhetővé.[14] A gyakorlatban előforduló olyan esetekre vonatkoznak az eltérések, amikor az erősen intézményesített garanciák ugyan nem állnak rendelkezésre, az adattovábbítás mégis legitimnek tekinthető. Bizonyos eltérések alkalmazásáról a tagállami felügyeleti hatóságokat értesíteni kell.

2.3.1. A megfelelőségi határozat

A GDPR 45. cikkének megfelelően az Európai Bizottság határozatban állapítja meg egy harmadik országról, hogy az megfelelő védelmi szintet biztosít a személyes adatok tekintetében. A döntés egy adott államra, annak egy területére vagy ágazatára is vonatkozhat.

A jogalkotási aktus meghozatalát számos körülmény mérlegelése előzi meg. A megfelelő védelmi szintre vonatkozó döntést megszerezni kívánó állammal részletes konzultáció zajlik a feltételek teljesüléséről. Ezeket maga a GDPR sorolja fel. Az elvárásrendszer három kategóriával írható le:
- az adott állam területén érvényesülniük kell a jogállami garanciáknak, így mindenekelőtt az emberi jogoknak; ebben a körben értékeli az Európai Bizottság az adatvédelmi szabályozást is, beleértve azt is, hogy az érintetteknek hatékony jogorvoslati rendszer áll rendelkezésre jogaik érvényesítése érdekében. Ez a kritérium tehát a jogállamiságra és a szabályozás minőségére vonatkozik;
- független adatvédelmi hatóság működik-e az adott államban, és az milyen módon járul hozzá a jog érvényesüléséhez (vizsgálati jogosultságok, tanácsadás stb.). Ez a kritérium az adatvédelmi intézményrendszer oldaláról vizsgálja a védelem körülményeit;
- az adott állam nemzetközi kötelezettségvállalásait is vizsgálják annak körében, hogy milyen módon lehet kikényszeríteni az Európai Unió elvárásait.

A Schrems-ügy nyomán került a GDPR szövegébe az a kitétel, amely szerint a megfelelő védelem szintjét rendszeres időközönként, legalább négyévente felül kell vizsgálni. A rendszeres felülvizsgálattól függetlenül az Európai Bizottságnak folyamatosan figyelemmel kell kísérnie azokat a fejleményeket, amelyek a megfelelőségi határozat végrehajtását érinthetik.[15]

---

11 Ebben az esetben is elvárás, hogy az ilyen megállapodások az érintettek számára érvényesíthető és tényleges jogaira vonatkozó rendelkezéseket tartalmazzanak [GDPR (3) bekezdés b) pont].

12 A GDPR 63. és 64. cikkének megfelelően.

13 A GDPR 48. cikke alapján.

14 Ezt az esetkört a GDPR 49. cikke sorolja fel, a felsorolás taxatív.

15 A GDPR 45. cikkének (4) bekezdése rendelkezik erről.

2.3.1.1. A megfelelő védelmi szint garantálásának elmulasztása és annak következményei

Ha a Bizottság meggyőződik a védelmi szintre vonatkozó körülmények megváltozásáról, tehát arról, hogy az adott állam (vagy annak területe, illetve ágazata) már nem biztosítja a megfelelő védelmi szintet, határozatát hatályon kívül helyezi, módosítja vagy felfüggeszti.[16]

Az Európai Bizottság megfelelőségi határozatának visszavonása, felfüggesztése, illetve módosítása esetén ha egyébként létezik más olyan hatályos jogi eszköz (például kötelező erejű vállalati szabályok), amely az adattovábbítás kapcsán a védelem szintjét szavatolja, akkor önmagában a bizottsági határozat hatályon kívül helyezése az adatforgalom jogszerűségét nem befolyásolja. Abban az esetben azonban, ha az adattovábbítás kapcsán a védelmi szintet más jogi eszköz nem biztosította, úgy az Európai Unióból a harmadik országba személyes adat jogszerűen nem továbbítható.

A GDPR alkalmazását megelőzően az Európai Bizottság számos olyan határozatot hozott, amelyben harmadik országok esetében állapították meg a megfelelő védelmi szintet.[17] A GDPR ezeket a jogalkotási aktusokat nem tekinti semmisnek, hanem azokat mindaddig hatályosnak tekinti, amíg módosításukra, felváltásukra vagy hatályon kívül helyezésükre sor nem kerül.[18]

2.3.1.2. Megfelelőségi határozat hatályon kívül helyezése az Egyesült Államok vonatkozásában – az Európai Unió Bíróságának ítélete a Schrems-ügyben

A GDPR 44. cikke fogalmazza meg azt az általános elvárást, amely szerint harmadik országba irányuló adattovábbítás, illetve az adatok harmadik országbeli további kezelése csak a rendelet valamennyi követelményének érvényesülése esetén valósulhat meg. Szintén általános elvárás, hogy a GDPR vonatkozó fejezetének valamennyi rendelkezését alkalmazni kell annak érdekében, „hogy a természetes személyek számára e rendeletben garantált védelem szintje ne sérüljön”.[19]

A megfelelő védelmi szint fogalma és követelménye nem új az Európai Unió jogában, az 1995-ös adatvédelmi irányelv szintén szabályozta azt. Annak megítélésekor, hogy az adott harmadik ország megfelelő védelmet biztosít-e, az irányelv alapján figyelembe kellett venni a továbbított adatok jellegét, a tervezett adatfeldolgozási művelet célját, időtartamát, a kiindulási és a célországot, a harmadik országban hatályos általános és ágazati jogrendet, valamint az adott országban érvényesülő szakmai szabályokat és biztonsági intézkedéseket.[20] Annak vizsgálatát, hogy mindezek a szempontok az Amerikai Egyesült Államok vonatkozásában érvényesülnek-e, a Maximiliam Schrems és az ír adatvédelmi biztos (Data Protection Commissioner) között zajló előzetes döntéshozatali eljárásban végezte el az Európai Unió Bírósága.[21]

A Bíróság ítéletében arra a következtetésre jutott, hogy adatoknak az Egyesült Államokba való továbbítása esetén nagyon tág körben, így a nemzetbiztonsággal, a közérdekkel vagy a bűnüldözési érdekkel összefüggő jogi kötelezettségeknek is elsőbbségük van a Safe Harbor elvekkel szemben. Ütközés esetén tehát az adatvédelmet szolgáló elveket az amerikai adatkezelőnek figyelmen kívül kell hagynia annak érdekében, hogy az Egyesült Államok jogszabályainak megfeleljen. A Bizottság határozata nem utal semmilyen jogi garanciára, amely az Európai Unióból importált adatok védelmét

---

16 Ebben az esetben is részletes elemzés előzi meg a döntéshozatalt, gyakorlatilag a megfelelőségi határozatot megelőző eljárás zajlik le, többfordulós tárgyalásokat is magában foglalva.

17 2000-ben Magyarország és Svájc, 2001-ben Kanada, 2003-ban Argentína és Guernsey, 2004-ben Man szigete, 2008-ban Jersey, 2010-ben Andorra és Feröer szigetek, 2011-ben Izrael Állam, 2012-ben az Uruguayi Keleti Köztársaság és Új-Zéland tekintetében állapította meg az Európai Bizottság a megfelelő védelmi szint meglétét.

18 A GDPR több más esetben is alkalmazza ezt az áthidaló, folyamatos jogalkalmazást lehetővé tevő megközelítést. A megfelelőségi határozatok folyamatos hatályáról a 45. cikk (9) bekezdése rendelkezik.

19 A GDPR 44. cikkének utolsó mondata szerint.

20 A kritériumokat a 95/46/EK irányelv 25. cikkének (2) bekezdése határozza meg.

21 C-362/14. számú ügy, Maximiliam Schrems és a Data Protection Commissioner között, a Digital Rights Ireland Ltd. részvételével; az ítélet 2015. október 6-án született.

szolgálná az Egyesült Államok jogrendjében. Az ilyen jogsértések kapcsán igénybe vehető jogi védelemre maga a határozat sem tartalmaz rendelkezést. Ennek következtében az európai jogalanyok nemcsak a közigazgatási vagy bírósági jogorvoslat lehetőségétől esnek el, de még az sem világos, hogy milyen módon gyakorolhatják érintetti jogaikat.[22]

Az Európai Alapjogi Charta 7. és 8. cikkében garantált jogok korlátozása esetén világos és pontos szabályokat kell megállapítani az egyének hatékony védelme érdekében, emellett a „feltétlenül szükséges" kritériumot is tiszteletben kell tartani. Ez utóbbi nem érvényesül, ha általános felhatalmazást nyújt az Unió jogalkotási aktusa az Egyesült Államokba exportált adatok korlátozás és válogatás nélküli kezelésére. Az olyan jogszabály, amely a hatóságok számára általános hozzáférést biztosít az elektronikus kommunikáció tartalmához, sérti a 7. cikkben rögzített, magánélethez való jog lényegét. Hasonló következtetésre kell jutni a hiányzó jogorvoslat és joggyakorlási lehetőségek kapcsán is.[23]

A 95/46/EK irányelv szerint az Európai Bizottságnak a megfelelőségi határozat elfogadása során meg kell győződnie arról, hogy a harmadik ország a hazai szabályozása és a nemzetközi kötelezettségvállalása alapján valóban az Európai Unió szabályozásával lényegében megegyező rezsimet hozott létre. A Bíróság arra a következtetésre jutott, hogy ezt a Bizottság be sem mutatta a határozatban, ezt a határozat nem is állapítja meg, ennek megfelelően más nem is következhet az elemzésből, mint hogy kimondja a 2000/520 számú határozat érvénytelenségét. A súlyos jogalkotási hibára tekintettel a Bíróság szerint nem is volt szükség a Safe Harbor elvek részletes tartalmi vizsgálatára.

2.3.1.3. A Safe Harbor határozat érvénytelenségének következményei

Az Európai Unió Bíróságának ítélete azzal járt, hogy az Egyesült Államokba irányuló adattovábbítások jogalapjaként a megfelelőség ezen módjára hivatkozni már nem lehetett, más módon kellett szavatolni a védelmi szintet. Erre szolgálhattak például a kötelező erejű vállalati szabályok vagy a szerződéses kikötések.

Az érvénytelenített Safe Harbor jogi keret helyébe az Egyesült Államok és az Európai Unió tárgyalásai során kidolgozott ún. EU–USA Adatvédelmi Pajzs megállapodás lépett, amelynek jogi formája európai oldalon ismét bizottsági határozat.[24]

2.3.1.4. A Privacy Shield (Adatvédelmi Pajzs) határozat

Az Európai Bizottság új határozata orvosolni kívánta a Safe Harbor hiányosságait, és ezért több ponton továbbfejlesztette azt. Az Adatvédelmi Pajzs rögzíti az adatvédelmi elveket,[25] amelyek az öntanúsítást követően azonnal alkalmazandóvá válnak.[26] A regisztráció menete a korábbihoz hasonlóan a Kereskedelmi Minisztériumnál[27] zajlik. Jelentős változás az érintetti joggyakorlás és a jogorvoslati lehetőségek bővítése.

Ahogyan a Safe Harbor rendszer ideje alatt, a Privacy Shield esetében is korlátozhatók az adatvédelmi elvek abban az esetben, ha nemzetbiztonsági, bűnüldözési vagy egyéb közérdekű célból

---

22 Így például milyen módon élhetnek a hozzáférés jogával, vagy milyen eljárás keretében érvényesíthetik az adatok helyesbítéséhez vagy törléséhez való jogukat.

23 Az ítélet 92–95. pontjai szerint.

24 A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU-USA adatvédelmi pajzs által biztosított védelem megfelelőségéről.

25 A tájékoztatás elve, az adatok sértetlensége és a célhoz kötöttség elve, az eredetitől eltérő új célú adatkezelések esetében a választási lehetőség (kívülmaradás) elve, a biztonság elve, a hozzáférés elve, a jogorvoslat, végrehajtás és felelősség elve, a harmadik fél részére történő adattovábbításért való elszámoltathatóság elve.

26 Privacy Shield határozat (17) preambulum bekezdésének első mondata szerint.

27 Department of Commerce.

szükséges az Európai Unióból továbbított személyes adatokhoz való hozzáférés. Az ilyen jellegű hozzáférést és felhasználást azonban csak korlátok között alkalmazzák az Egyesült Államok hatóságai, és külön, független szereplőt, ombudsmant neveznek ki a felügyeleti mechanizmus hatékonysága érdekében.[28]

Az Adatvédelmi Pajzs fontos újítása, hogy rendszeres, évente végrehajtott felülvizsgálatot vezet be.

Mindezek alapján az Európai Bizottság határozatában arra a következtetésre jutott, hogy az Egyesült Államok megfelelő védelmi szintet biztosít az EU–USA adatvédelmi pajzs keretében az Unióból az öntanúsított szervezetekhez továbbított személyes adatok tekintetében.

2.3.2. Megfelelő garanciák alapján történő adattovábbítások

A megfelelő garanciák esetében az adatkezelőkre, illetve adatfeldolgozókra hárul annak feladata, hogy a személyes adatok védelmének feltételeit megteremtsék. A GDPR elvárása az, hogy ezek a garanciák az „Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítanak az érintettek számára".[29] Ezek a garanciák magukban foglalják a hatékony bírósági vagy közigazgatási jogorvoslatot, és a kártérítéshez való jogot is. A megfelelő garanciák esetében mindig fontos szerepet játszanak a tagállami adatvédelmi felügyeleti hatóságok.

Az alábbiakban a megfelelő garanciák egyes eszközeit mutatjuk be részletesen.

2.3.2.1. A kötelező erejű vállalati szabályok (BCR) a GDPR-ban

A vállalkozáscsoporton belül van mód arra, hogy a tagállami adatvédelmi hatóság által jóváhagyott[30] kötelező erejű vállalati szabályok révén garantálják a határon átnyúló adattovábbítás tekintetében az adatok védelmét. A BCR-ek jellemzően olyan vállalatcsoportok[31] esetében hasznosak, amelyek úgy folytatnak határon átnyúló tevékenységet, hogy az érintett országok egy része az Európai Unión belül, másik része pedig az Unión kívül helyezkedik el.

A vállalati szabályoknak[32] be kell mutatniuk magát a szervezetet, így a szervezeti felépítést és az elérhetőségét.[33] Részletesen ismertetniük kell a vállalati működés rendjét, kitérve az adattovábbításokra és ezek sorozatára, a továbbított adatok és az érintettek kategóriáira, az adatkezelések céljára, a címzett országokra, az esetleges újbóli továbbítás feltételeire. A vállalati szabályok jogi természetét is be kell mutatni, így különösen azt, hogy a szabályzat belső és külső tekintetben is jogilag kötelező a vállalatcsoport tagjaira nézve.

Az adatalanyok számára is ismertté kell tenni azokat a szabályokat, amelyek az ő szempontjukból jelentősek: tájékoztatást kell nyújtani az érintetti jogokról és e jogok gyakorlásának módjáról, a jogorvoslati lehetőségről. Első helyen a panasztétel lehetősége szerepel, továbbá a hatósági és a bírósági jogérvényesítésen túl a kártérítéshez való jogról is tájékoztatni kell az érintetteket.

A kötelező erejű vállalati szabályok összetett jogi környezetben érvényesülnek, több jogi szabályozás területén és számos szereplő részvételével. Fogalmazhatunk úgy is, hogy a megfelelő

---

28 A Privacy Shield határozat (65) preambulum bekezdése szerint az ombudsman független a hírszerzéstől.

29 A GDPR (108) preambulum bekezdésének harmadik mondata szerint.

30 A felügyeleti hatóság a kötelező erejű vállalati szabályokat a GDPR egységességi mechanizmusának megfelelően hagyja jóvá.

31 A magyar Polgári Törvénykönyv III. könyvében VI. cím alatt definiálja a vállalatcsoport fogalmát. Ez a fogalom alkalmazandó uniós összefüggésben is.

32 A szabályok tartalmát részletesen a GDPR 47. cikke határozza meg.

33 Az itt tárgyalt valamennyi szabály jól illeszkedik a GDPR 5. cikkének (2) bekezdésében megfogalmazott elszámoltathatóság elvéhez.

garanciák esetében számolni kell a jogállami deficittel. Ez a közeg különös körültekintést indokol, erre tekintettel épített be az uniós jogalkotó további olyan garanciákat, amelyek egyébként a többi adatkezelés esetében alapvető elvárásként nem jelentkeznek:

- az egyik uniós tagállamban tevékenységi hellyel rendelkező adatkezelőnek felelősségét el kell ismernie abban az esetben, ha a szabályokat az unióban tevékenységi hellyel nem rendelkező tag megsérti.
- ki kell dolgozni a kötelező erejű vállalati szabályoknak való megfelelés ellenőrzésére szolgáló mechanizmusokat;
- az adatvédelmi felügyeleti hatóságnak be kell jelenteni a harmadik országban érvényes olyan jogi előírásokat, amelyek várhatóan hátrányosan érintenék a kötelező vállalati szabályok által előírt garanciákat.

A bemutatott pótlólagos garanciák azt hivatottak szolgálni, hogy az Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat biztosítsanak az érintettek számára.

A vállalati szabályokat minden esetben az egyik uniós tagállami adatvédelmi felügyeleti hatóság hagyja jóvá formálisan, tartalmában azonban a hatóságok közötti együttműködés révén születik meg a jóváhagyás az egységességi mechanizmus keretében.[34]

2.3.2.2. Az Európai Bizottság által elfogadott általános adatvédelmi kikötések

A GDPR szabályozása a rugalmasság érdekében vegyíti a kötelező és a szabadon választható jogi eszközöket. Az általános adatvédelmi kikötések magánfelek által alkalmazhatók. Nem ez az egyetlen módja a megfelelőség biztosításának, mindazonáltal igénybevétele esetén jogbiztonságra számíthatnak a felek, hiszen egy olyan szerződéses kikötésrendszert alkalmaznak, amelynek megfelelőségét az Európai Bizottság állapította meg. Attól a ponttól, hogy a szerződéses kikötéseket alkalmazzák, értelemszerűen jogilag kikényszeríthető jogok és kötelezettségek származnak a jogviszonyból.

A kötelező erejű vállalati szabályokkal összevetve jelentős különbség, hogy a jogalkotó nem csupán a szerződések tartalmára nézve ad iránymutatást, mint a BCR-ek esetében, hanem szövegszerű, módosítást nem igénylő módon átvehető szerződéses kikötéseket kínál. Az Európai Bizottság közvetlenül alkalmazandó határozatokat fogadott el ezen a téren, amelyek tehát a tagállami jogszabályoktól függetlenül érvényesülnek.

Két viszonylatot szabályoz a Bizottság:

- Az Európai Unióban tevékenykedő adatkezelő személyes adatokat továbbít egy Unión kívül működő adatkezelő számára. Erre vonatkozik a 2001/497/EK,[35] valamint a 2004/915/EK[36] számú bizottsági határozat;
- Az Európai Unióban tevékenykedő adatkezelő személyes adatokat továbbít egy Unión kívül működő adatfeldolgozó számára. Ezt az esetkört szabályozza a 2010/87/EU számú bizottsági határozat.[37]

---

[34] A harmadik országba irányuló adattovábbítás terén a teljes harmonizációra törekvés jogalkotói szándéka nyilvánul itt meg, amely a védelem szintjének megőrzése szempontjából is jelentős.

[35] A Bizottság határozata (2001. június 15.) a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről.

[36] A Bizottság határozata (2004. december 27.) a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről.

[37] A Bizottság határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről. A 2002/16/EK számú határozat szintén erre a területre vonatkozott, azonban azt a 2010-es határozat hatályon kívül helyezte.

A bizottsági határozatok funkciója az, hogy a harmadik országok felé megvalósuló adattovábbítások során a felek jogai és kötelezettségei tisztázottak legyenek, az érintettek jogai pedig érvényesüljenek.

A határozatokban leírt szerződéses kikötések valójában az európai adatvédelmi szabályozás kivonatát tartalmazzák azzal, hogy az egyes műveletek leírása révén testre szabott dokumentumot írnak alá a felek.

A határozatok mellékletét képező szerződéses kikötések kiegészíthetők üzleti jellegű megállapodásokkal, azonban azokat módosítani nem lehet. Az adatkezelő–adatkezelő viszonylatban sorra kerülő adattovábbítások esetében két szerződéses csomag közül is választhatnak a szerződő felek. E két csomagot azonban nem lehet összevonni, vagy az egyik (a 2001/497/EK számú határozatban foglalt), vagy a másik (a 2004/915/EK számú határozatban foglalt) szöveg alkalmazandó. Az adatkezelő–adatfeldolgozó viszonylatban alternatív csomag nincsen, az Európai Bizottság csak egy kikötésrendszert dolgozott ki és bocsátott az adatkezelők részére.

2.3.2.2.1 Felelősség, kártérítés

A felelősség kétirányú szabályozását találjuk a vonatkozó bizottsági határozatokban. A jogalkotó rendezi az adatátadó (uniós adatkezelő) és az adatátvevő (Unión kívüli adatkezelő vagy adatfeldolgozó) felelősségét az érintettek felé, továbbá a felek egymás közötti felelősségét.

Az érintett irányában fennálló felelősség főszabálya az egyetemlegesség. Az adatok átadójának és átvevőjének „egyetemleges felelősséget kell vállalniuk” az adatalanyokra vonatkozó kikötés „bármilyen megsértéséből eredő károkért”.[38] Akkor mentesülhetnek a felelősség alól, ha bizonyítják, hogy egyikük sem tartozik felelősséggel az adatalanyokra vonatkozó kikötés megsértéséért.[39]

A felelősség rendezésének szükségessége a szerződés sajátosságaiból is fakad. A személyes adatok biztonságáért mind az adatátadó, mind az adatátvevő felel. Az adatátvevő az Európai Unión kívül tevékenykedik, ezért elengedhetetlen, hogy a technikai és szervezési biztonsági intézkedések megtételére való kötelezettség és az ehhez tartozó felelősségvállalás is része legyen a szerződéses kikötéseknek. A megtett biztonsági intézkedéseknek alkalmasnak kell lenniük többek között az adatok véletlen vagy jogellenes megsemmisülése, a véletlen elvesztés, megváltoztatás elleni védelemre. Az intézkedések alapjául szolgálnak a kockázatok, az aktuális körülmények (technológia fejlettsége) és a költségek, az arányosság mindezek fényében ítélendő meg.[40]

2.3.3. Különös helyzetekben biztosított eltérések

A GDPR az adatok védelme érdekében a harmadik országok viszonylatában következetes rendszert alkalmaz. A megfelelőségi határozat és az ún. megfelelő garanciák hiányában eltéréseket enged szűk körben az adatok továbbítása terén, ennek garanciarendszerét mutatjuk be az alábbiakban.[41] Az eltérések szűken értelmezendők, el kell kerülni, hogy a kivételeket túl gyakran alkalmazzák az adatkezelők, és ilyen módon a kivétel váljon szabállyá.[42]

38 2001/497/EK számú határozat (18) preambulum bekezdése és a melléklet 6. pontja szerint.

39 2001/497/EK számú határozat mellékletének 6. 1. pontja szerint.

40 2010/87/EU számú határozat mellékletének 4. d) pontja szerint.

41 Az itt tárgyalt 49. cikkről az Európai Adatvédelmi Testület első, 2018. május 25-én tartott ülésén iránymutatást fogadott el Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 címmel. A szövegben testületi iránymutatásként hivatkozunk rá.

42 Testületi iránymutatás, 4. o.

2.3.3.1. Az érintett kifejezett hozzájárulása

A rendelet az információs önrendelkezési jog logikájának megfelelően első helyen az érintett hozzájárulását említi eltérésként, az adatalany mérlegelésére bízva az adattovábbítás megengedhetőségét.

Az érintett hozzájárulását a GDPR általánosságban szabályozza, egyrészt definícióként rögzíti, másrészt külön szabályokat állapít meg rá nézve.[43] A harmadik országba irányuló adattovábbítás esetében kifejezett hozzájárulásra van szükség, amely elvárás csak néhány esetben fordul elő a GDPR-ban.[44]

Az érintett nem „általában" járul hozzá adatok továbbításához, hanem a konkrét transzferhez kell a hozzájárulását beszerezni. Erre a nyilatkozatra csak az érintett tájékoztatását követően kerülhet sor. Amennyiben a tájékoztatás nem teljes, úgy az adattovábbítás jogalapja is hiányzik, hiszen amiről az érintett nem tud, azt értelemszerűen a hozzájáruló nyilatkozata sem foglalhatja magában.

2.3.3.2. Szerződés teljesítése

A szerződésben az érintett lehet, hogy maga is fél, ilyenkor az adatkezelő és az érintett közötti szerződés teljesítéséhez vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges az adatok továbbítása. Az adattovábbítás jogszerűsége körében meg kell vizsgálni, hogy a továbbítandó adatok valóban szükségesek-e az említett célokból, és megfelelően szoros kapcsolat mutatható-e ki a szerződés és az adatok között.[45] Ha nincs közvetlen és objektív kapcsolat a szerződés célja és az adatok továbbítása között, akkor más jogalapot kell keresni a transzfer jogszerűvé tétele érdekében.

Akkor is megnyílik az eltérés alkalmazásának lehetősége, ha az adattovábbítás az adatkezelő és más személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges.

2.3.3.3. Jogi igények előterjesztése

Szintén megfelelő alapja lehet az adattovábbításnak, ha a harmadik országba jogi igény előterjesztése, érvényesítése és védelme miatt szükséges az adatok továbbítása. Ez vonatkozhat valamely polgári, közigazgatási jogi vagy büntetőjogi igényre is. Tipikusan azok a helyzetek tartoznak ebbe a körbe, amikor valakinek védekeznie kell egy hatósági eljárásban, vagy valamilyen eljárás során igénybe vehető kedvezmény, esetleg mentesülés érdekében nélkülözhetetlen a továbbított adatok felhasználása.[46]

2.3.3.4. Fontos közérdek

Az adatok továbbításának alapja lehet olyan fontos közérdek, amelyet az uniós jog vagy az adatkezelőre alkalmazandó tagállami jog elismer. Nem absztrakt célok, hanem konkrét célkitűzések képezhetik alapját e jogszabályhely alkalmazásának.

---

43 A hozzájárulás fogalmát a GDPR 4. cikk 11. pontja, míg a hozzájárulás feltételeit a 7. cikk határozza meg.

44 Az adatok jogszerű kezeléséhez az érintett kifejezett hozzájárulására van szükség a személyes adatok különleges kategóriáinak kezelésekor (GDPR 9. és 10. cikk), továbbá az automatizált egyedi döntéshozatal során (beleértve a profilalkotást is) (GDPR 22. cikk).

45 Ez az ún. szükségességi teszt, amit a testületi iránymutatás elemez (9. o.).

46 Így például egy trösztellenes vizsgálat során a pénzbírság elkerülése érdekében.

2.3.3.5. Létfontosságú érdek

A létfontosságú érdek az adatkezelés jogalapjaként az általános szabályok között is megjelenik.[47] Ez az eltérés akkor alkalmazható, ha valóban életveszélyről, a testi épséget, egészséget veszélyeztető helyzetről van szó, és egyértelmű, hogy például az azonnali orvosi beavatkozás, az egyént érintő kockázatok elhárítása érdekében az adatvédelmi aggályokat az adott helyzetben figyelmen kívül kell hagyni.

Ez az eltérés nem alkalmazható minden egészségügyi kontextusban. Egészségügyi kutatás céljából továbbítandó adatok kapcsán például nem lehet rá hivatkozni, hiszen ilyen esetben az az elvárás, hogy valamely szükséghelyzetben lévő személynek a diagnózisához van szükség az adatra, nem érvényesül.[48]

2.3.3.6. A nyilvánosság tájékoztatását szolgáló nyilvántartásból származó adatok

Az általános szabályokhoz képest enyhébb megítélés alá esik a szabályozott módon bárki számára hozzáférhető nyilvántartásokból származó adatok harmadik országba irányuló továbbítása. Itt az uniós vagy a tagállami jog által szabályozott olyan nyilvántartásokról van szó, amelyek célja a nyilvánosság tájékoztatása akár olyan módon, hogy bárki, jogos érdek igazolása nélkül, vagy jogos érdek igazolása mellett férhet hozzá az adatbázisban rögzített bizonyos, lekért adatokhoz. Amennyiben a jog által egyébként támasztott feltételek teljesülnek, akkor a harmadik országba irányuló adattovábbítás esetében sem kell további követelményeknek megfelelni. Az is előfordulhat, hogy a jogos érdekét igazoló személy harmadik országban tartózkodik, vagy ott honos, ez azonban nem akadálya az adatok továbbításának, hiszen a jogos érdeket igazolták, és egyébként az adatok pedig bárki számára hozzáférhetők egyébként is.[49]

A rendelet beépít egy további garanciát az adatok védelme érdekében. E szerint az adattovábbítás nem érintheti a nyilvántartásban szereplő személyes adatok összességét, és ehhez hasonlóan nem érintheti a személyes adatok kategóriáinak összességét.[50]

2.3.3.7. Érdekmérlegelés – kényszerítő erejű jogos érdeken alapuló adattovábbítások

Az eltérések a fentiekben bemutatott módon kivételt képeznek a fő szabályhoz képest. Amennyiben a harmadik országba irányuló adattovábbítás az eddig tárgyalt kategóriákba nem sorolható be, úgy a rendelet további szűk körben enged eltérést az általános szabályhoz képest, ennek azonban számos feltétele van. Ebben az esetben az adatkezelőnek, tehát az adatok Európai Unióban működő továbbítójának egy érdekmérlegelési tesztet kell elvégeznie. Az érdekmérlegelés során azt kell megvizsgálni, hogy az adattovábbítást indokoló kényszerítő erejű jogos érdek túlnyomó-e az érintett érdekeivel szemben. Az adatkezelőnek e mérlegelés során az adattovábbítás minden körülményét meg kell vizsgálnia. Az adatkezelő oldalán olyan kényszerítő erejű jogos érdeket kell tudni bemutatni, amelyeknek valóban elsőbbséget kell élvezniük az érintetti érdekekkel szemben. Ilyen lehet például az az eset, amikor az adatkezelő szervezet kénytelen a saját érdekeinek védelme céljából adatokat továbbítani külföldre, hogy közvetlenül fenyegető kárt előzzön meg, vagy egy közigazgatási bírsággal fenyegető eljárásban azt felhasználhassa.[51]

További feltétele az adatok továbbításának, hogy az nem ismétlődő, és csak korlátozott számú érintettre vonatkozik.

---

47 A GDPR 6. cikk (1) bekezdés d) pontja szerint az adatkezelés akkor jogszerű, ha többek között az érintett vagy egy másik természetes személy létfontosságú érdekének védelme miatt szükséges.

48 Testületi iránymutatás, 13. o.

49 A GDPR 49. cikk (2) bekezdésének utolsó fordulata szerint.

50 A 49. cikk (2) bekezdésének első mondata szerint.

51 Testületi iránymutatás, 15. o.

Az adatkezelőnek megfelelő garanciákat kell nyújtania a továbbított személyes adatok védelme tekintetében. Fel kell mérnie és minimalizálnia kell azokat a kockázatokat, amelyek a harmadik országban az érintett jogait és érdekeit sérthetik. Ilyen intézkedés lehet az adatok mielőbbi törlése vagy anonimizálása, illetve az adatok felhasználásának céljait is korlátozni lehet.

A rendelet azt is előírja a tárgyalt eltérés kapcsán, hogy az adattovábbítás csak korlátozott számú érintettre vonatkozhat.

A rendelet végül két tájékoztatási kötelezettséget is előír: értesíteni kell az adatvédelmi felügyeleti hatóságot, továbbá az adatkezelő az érintettet is tájékoztatja az adattovábbításról.

Az adatvédelmi hatóság tájékoztatása nem engedély beszerzésére irányul, csupán tájékoztatásról van szó. E tájékoztatásnak is van garanciális szerepe, hiszen a hatóság ilyen módon értesül a továbbításról, és szükség esetén meg tudja vizsgálni az adattovábbítás körülményeit.

Az érintett az adatok kezeléséről a rendelet 13. és 14. cikke szerint tájékoztatásra jogosult. A tájékoztatásnak ki kell terjednie a kényszerítő erejű jogos érdek bemutatására is.

2.3.3.8. Általános elvárások, valamint pótlólagos követelmények egyes eltérések esetében

2.3.3.8.1 Közhatalmi szervekre vonatkozó kivételek

Az eltérések a közhatalmi szervek esetében nem alkalmazható akkor, amikor

- az adattovábbítás jogalapja az érintett hozzájárulása,
- az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, illetve a szerződést megelőző intézkedések végrehajtásához szükséges,
- az adattovábbítás az adatkezelő és valamely más személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges,
- az adatkezelő kényszerítő erejű jogos érdekében szükséges.

A kivételszabály akkor érvényesül, amikor a közhatalmi szervek közhatalmi jogosítványai gyakorlása során járnak el. Abban az esetben, amikor magánjogi jogviszonyok alanyaként jelennek meg, értelemszerűen rájuk is az általános szabályok vonatkoznak.

2.3.3.8.2. Tagállami jogban előírt tilalom

A GDPR-t kisegítő szabályként, illetve pótlólagos garanciaként említhetjük azt, hogy az Uniónak, valamint bármely tagállamnak lehetősége van arra, hogy bizonyos kategóriákba tartozó személyes adatok valamely harmadik országba irányuló továbbítását megtiltsa. Az ilyen tagállami szabályt az Európai Bizottságnak be kell jelenteni.

Összefoglalva azt mondhatjuk el a bemutatott eltérésekről, hogy vagy az érintett hozzájárulásával kerül sor az adatok továbbítására, vagy olyan esetekben, amikor valamely érdek túlnyomó az érintett (magán)érdekeivel szemben. Ez megjelenhet szerződésben, uniós vagy tagállami jogban nevesített közérdekben, jogi igény előterjesztésének kényszerében, létfontosságú érdek védelmében, továbbá kényszerítő erejű jogos érdek érvényesítése céljából. A köz tájékoztatására létrehozott nyilvántartások esetében a jogalkotó az érintett érdekeit általában nem tekinti túlnyomónak az adatok továbbítása tekintetében, csupán néhány garanciális szabály érvényesítését várja el a jogalkalmazótól.

2.3.4. Az uniós jog által nem engedélyezett adattovábbítás és közlés

A rendelet 48. cikke szerint „valamely harmadik ország bíróságának bármely olyan ítélete, illetve közigazgatási hatóságának bármely olyan döntése, amely valamely adatkezelő vagy adatfeldolgozó számára személyes adatok továbbítását vagy közlését írja elő, kizárólag akkor ismerhető el vagy hajtható bármely módon végre, ha az az adatok megismerését igénylő harmadik ország és az Unió vagy egy tagállama között létrejött, hatályos nemzetközi megállapodáson, például kölcsönös jogsegélyszerződésen alapul". Az adattovábbítás során a rendelet harmadik országokba irányuló adattovábbításait szabályozó V. fejezetét figyelembe kell venni, az ott írt szabályok és garanciák nem sérülhetnek.

Ez a cikk is egy kisegítő szabály, amely a jogalkalmazás során tömegével előforduló esetekre nyújt iránymutatást. A rendelet szabályozni kívánja a harmadik országok bírósági, illetve hatósági döntésein alapuló adattovábbításokat. A fő szabályokat a fejezet korábbi rendelkezései rögzítik, a 48. cikk csupán azokra az esetekre nyújt szabályozást, amikor egy harmadik ország bírósági vagy hatósági döntése egy Unióban tevékenykedő adatkezelőt kötelez személyes adatok továbbítására.

Tekintettel arra, hogy egy harmadik ország jogszabálya, valamint az azon alapuló döntés határon átnyúló alkalmazása sértheti a nemzetközi jogot, és leronthatja az Unióban biztosított védelmi szintet, a rendelet további feltételt támaszt az ilyen adattovábbításokkal szemben. Nem utasítja el általánosságban az ilyen adatigények teljesíthetőségét, de csak akkor tartja megengedhetőnek, ha az egyébként megfelel az V. fejezet előírásainak. Ez a feltétel akkor teljesül többek között, ha az adatok igénylése nemzetközi megállapodáson alapul. Ilyen megállapodás lehet a kölcsönös jogsegélyszerződés. Nemzetközi megállapodás hiányában is alkalmazható a fent elemzett, fontos közérdekre vonatkozó eltérés, azzal a fontos megjegyzéssel, hogy ezt a közérdeket az uniós vagy tagállami jognak el kell ismernie.

2.3.5. Adatvédelmi felügyeleti hatóságok szerepe

A harmadik országba irányuló adattovábbítások kapcsán a jogalkotó elsősorban az Unióban működő adatvédelmi hatóságok szerepével számol, hiszen a nem megfelelő védelmi szintet pótló garanciákat biztosít a szerződéses kikötések rendszere. E hiányosságok között pedig az adatvédelmi hatóságok hiánya vagy nem megfelelő működése is előfordulhat. Az uniós hatóságok szerepét kiemeli az a körülmény is, hogy az adattovábbítás kiindulópontja mindig egy adott tagállam. A továbbítás jogszerűségének vizsgálatára pedig az adott tagállami adatvédelmi felügyeleti hatóság jogosult.[52]

Az Unióban tevékenykedő adatkezelő (adatátadó) adatvédelmi hatósággal való együttműködésének kötelezettsége a GDPR-ból fakad, azt nem szükséges a szerződéses kikötések között külön szabályozni. A harmadik országbeli adatkezelő vagy adatfeldolgozó esetében a védelem szintjének megőrzése érdekében elengedhetetlen kötelezni a szerződő felet arra, hogy az adatvédelmi hatóság megkeresése esetén „azzal együttműködik és betartja" az adatok kezelésével összefüggésben megfogalmazott javaslatokat.[53] Az adatátadó székhelye szerinti hatóság, bíróság jogerős határozatát a felek magukra nézve kötelezőnek ismerik el.[54]

[52] 2001/497/EK számú határozat (7) preambulum bekezdése szerint.
[53] 2001/497/EK számú határozat mellékletének 5. c) pontja.
[54] 2004/915/EK számú határozat mellékletének V. pontja (II. csomag).

2.3.6. A harmadik országba irányuló adattovábbítás jövőbeni érvényesülése

A fentiekben részletesen elemeztük a harmadik országba irányuló adattovábbítások szabályozását és egyes eszközeit. A szabályozás több ponton kifejezetten számol a jövőbeni alkalmazkodás lehetőségével, így rendszeres felülvizsgálatot ír elő a megfelelőségi határozat vagy a kötelező erejű vállalati szabályok esetében. A területre jellemző marad egyfajta dinamizmus, ami több okból is ered. A szabályozás több ponton keretszabályozás csupán, és a konkrét, napi gyakorlatban érvényesülő szabályok nem a jogalkotó által létrehozott normák (így a magatartási kódexek esetében például). A harmadik országba irányuló adattovábbítások feltételeit a célországokban érvényesülő gyakorlat szintén alapvetően befolyásolja.

A GDPR V. fejezete a fenti megfontolásokra tekintettel a lehető legnagyobb mozgásteret nyújtja a jogalkalmazó és a jogalkotásba közvetett módon bekapcsolódó szereplők (adatkezelők, adatvédelmi felügyeleti hatóságok, Európai Adatvédelmi Testület) számára. Szükség is van erre a rugalmasságra, hiszen a harmadik országok viszonylatában az uniós szinten biztosított védelmi szint folyamatos kihívásoknak lesz kitéve. Ezek a kihívások egyes országokkal kapcsolatban közelebb állnak a konfliktusokhoz, semmint csupán szabályozási vagy technikai kérdések lennének csupán. A szabadkereskedelmi megállapodások elengedhetetlen részeként a megfelelőség elismerése elkerülhetetlen témája a nemzetközi egyeztetéseknek.

Minderre tekintettel a harmadik országba irányuló adattovábbítások szabályozása jó fokmérője lesz a magánszféra-védelem globális állapotának, és ütközési pontja az Európai Unió arra irányuló törekvésének, hogy az általa nyújtani kívánt védelmi szintet hogyan tudja megőrizni globális szinten is.

2.4. Személyes adatok harmadik országba történő továbbítása az Infotv.[55] alapján

Az Infotv. a GDPR hatálya alá nem tartozó adatkezelések esetére a fentiektől eltérő szabályokat határoz meg. Ezek vonatkoznak a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatkezelésekre. Az Infotv. meghatározza az adattovábbítás fogalmát is, amely az adat meghatározott harmadik személy számára történő hozzáférhetővé tételét jelenti.[56] Az adattovábbítás általános feltételeit a 8. §, míg a harmadik országban, továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítás feltételeit a 10–12. §-ok tartalmazzák. Az itt lefektetett szabályok eltérőek a GDPR V. fejezetétől, és külön szabályokat állapítanak meg a bűnüldözési célú adatkezelések esetére, ez szolgál ugyanis a 2016/680 számú ún. bűnügyi irányelv[57] V. fejezetének nemzeti jogba történő átültetésére.

Személyes adatokat az Infotv. hatálya alá tartozó adatkezelő vagy adatfeldolgozó harmadik országban vagy nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére akkor továbbíthat, ha a nemzetközi adattovábbításhoz az érintett kifejezetten hozzájárult; vagy a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, és annak során teljesülnek az adatkezelés Infotv. 5. §-ban előírt feltételei[58] és az adatok címzettje tekintetében a

[55] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[56] Infotv. 3. § 11. pont.

[57] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE (2016. április 27.) 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.

[58] Az Infotv. 5. §-a az adatkezelés jogalapjait, illetve általános feltételeit határozza meg.

személyes adatok megfelelő szintű védelme biztosított; vagy a nemzetközi adattovábbítás az Infotv.-ben meghatározott kivételes esetekben[59] szükséges.

Bűnüldözési célú adatkezelés esetén nemzetközi adattovábbításra a fent meghatározott feltételek teljesülése esetén is csak akkor kerülhet sor, ha

- az bűnüldözési célból szükséges,
- annak címzettje
  - bűnüldözési adatkezelést folytató szerv, vagy
  - nem bűnüldözési adatkezelést folytató szerv és a 11. § (3) bekezdésében meghatározott feltételek teljesülnek, és
- nemzetközi adattovábbítással érintett személyes adatnak valamely EGT-állam adatkezelőjétől történő átvétele esetén,
  - a nemzetközi adattovábbítást ezen személyes adatok tekintetében az EGT-állam adatkezelője vagy képviseletében eljáró más szerv vagy személy előzetesen jóváhagyta, vagy
  - a – közvetett adattovábbítás kivételével – a nemzetközi adattovábbítás Magyarország vagy valamely más EGT-állam alapvető érdekeit vagy ezen államok vagy harmadik ország közbiztonságát fenyegető súlyos és közvetlen veszély megelőzése érdekében szükséges és ez előző alpont szerinti előzetes jóváhagyás beszerzése ezen érdekek sérelme nélkül a nemzetközi adattovábbítást megelőzően nem lehetséges.

A megfelelő védelmi szint akkor tekinthető biztosítottnak, ha azt az Európai Unió kötelező jogi aktusa azt megállapítja, ilyen jogi aktus hiányában vagy alkalmazásának felfüggesztése esetén az érintetteknek az Infotv. 14. §-ban, a 22. §-ban és a 23. §-ban foglalt jogai érvényesítésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés alkalmazandó Magyarország és azon harmadik ország, illetve nemzetközi szervezet között, amelynek joghatósága kiterjed a nemzetközi adattovábbítás címzettjére, vagy az előzőekben meghatározott jogi aktus hiányában vagy alkalmazásának felfüggesztése esetén a nemzetközi adattovábbítást megelőzően az adatkezelő a személyes adatok továbbításának valamennyi körülményét megvizsgálta, és megállapította, hogy a személyes adatok megfelelő szintű védelme tekintetében megfelelő garanciák állnak fenn.[60]

Ilyen kivételes esetek, vagyis az érintett kifejezett hozzájárulása, illetve a megfelelő védelmi szint biztosításának hiányában akkor kerülhet sor adattovábbításra, ha

- az az érintett vagy más személy létfontosságú érdekeinek védelme érdekében szükséges;
- valamely EGT-állam vagy harmadik ország közbiztonságát közvetlenül és súlyosan fenyegető veszély elhárítása érdekében szükséges;
- egyedi ügyben, eseti jelleggel az adatkezelő által végzett vizsgálatok vagy eljárások hatékony és eredményes lefolytatása érdekében szükséges, és az nem jár az érintett alapvető jogainak aránytalan korlátozásával; vagy
- egyedi ügyben, eseti jelleggel az érintett vagy más jogi igényeinek előterjesztése, érvényesítése, illetve védelme érdekében szükséges, és az nem jár az érintett alapvető jogainak aránytalan korlátozásával.

Az Infotv. a bűnüldözési célú adatkezelésre vonatkozóan az ilyen, kivételes esetben történő adattovábbítás eseteit tovább részletezi, pontosítja.[61] Emellett az Infotv. bizonyos esetekre vonatkozóan külön nevesíti a továbbítást végző szerv részére a dokumentálás, illetve a Hatóság tájékoztatásának kötelezettségét.[62]

[59] Infotv. 11. § (1) bekezdés a)–d).
[60] Infotv. 10. § (4) bekezdés.
[61] Infotv. 11. (2)–(3) bekezdések.
[62] Infotv. 12. §.

3. MAGATARTÁSI KÓDEX

3.1. A magatartási kódex fogalma

A tagállamok, a felügyeleti hatóságok, a Testület és a Bizottság ösztönzik olyan magatartási kódexek kidolgozását, amelyek – a különböző adatkezelő ágazatok egyedi jellemzőinek, valamint a mikro-, kis- és középvállalkozások sajátos igényeinek figyelembevételével – segítik a GDPR helyes alkalmazását.[63]

A magatartási kódex egy olyan szabályzat, amelyet adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek dolgozhatnak ki abból a célból, hogy pontosítsák a GDPR alkalmazását.[64] A magatartási kódex praktikus, költséghatékony és hasznos eszköz, és segít az adatkezelőknek abban, hogy magasabb szintű adatvédelmi megfelelést érjenek el, és felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti a GDPR-ban meghatározott kötelezettségeit.

Amennyiben az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek, szervezetek úgy döntenek, hogy magatartási kódexet alkotnak, ez egyrészt lehetőséget ad arra, hogy egy közös szabályrendszerben megállapodjanak az általuk folytatott adatkezelésekre vonatkozóan, másrészt arra, hogy rögzítsék a jó gyakorlatokat. Az eszköz emellett lehetővé teszi, sőt ösztönzi a megalkotóit („a kódex felelőseit") arra, hogy figyelembe vegyék az azt alkalmazni kívánó, konkrét adatkezelői vagy adatfeldolgozói kör, például egy szektor vagy akár a kis- és középvállalkozások és az általuk végzett adatkezelések sajátosságait. A kódexnek ugyanis az egyik fő követelménye, hogy hozzáadott értéket képviseljen, és pontosítsa az általános adatvédelmi rendeletben előírt követelményeket. A kódexre úgy is lehet tekinteni, mint önszabályozó eszközre, amelyben az azt alkalmazó, illetve az ahhoz csatlakozó adatkezelők/adatfeldolgozók vállalják, hogy az általuk végzett adatkezeléseket az abban lefektetett szabályok, jó gyakorlatok szerint fogják végezni, illetve alávetik magukat az abban létrehozott ellenőrzési mechanizmusoknak.[65]

Jelentős előnye lehet a magatartási kódexnek, hogy bizalmat kelt az érintettekben az azt alkalmazó adatkezelők és adatfeldolgozók irányában, illetve segíti azt is, hogy a tagok által folytatott adatkezeléseket átláthatóvá tegye.

A magatartási kódex a GDPR alapján felhasználható arra, hogy megfelelő garanciákat teremtsen a harmadik országba történő adattovábbítás esetén, azzal a feltétellel, hogy a harmadik országban letelepedett adatkezelő vagy adatfeldolgozó szerződéses vagy egyéb, jogilag kötelező erejű eszközök révén kötelező erejű és kikényszeríthető kötelezettségvállalást tesz arra, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogaira vonatkozókat is.[66] A hivatkozott rendelkezések alapján azonban erre csak az olyan magatartási kódex használható fel, amely határon átnyúló jellegű, és a Testület véleményét követően az Európai Bizottság végrehajtási aktus útján úgy határozott, hogy általános érvénnyel rendelkezik.

---

63 GDPR 40. cikk (1) bekezdés.

64 GDPR 40. cikk (2) bekezdés.

65 Európai Adatvédelmi Testület 1/2019 iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről.

66 GDPR 40. cikk (3), illetve 46. cikk (2) bekezdés e) pontja.

A magatartási kódex rugalmas eszköz, mivel az azt létrehozó szervezet eldöntheti, hogy mire terjed ki: lehetnek szűken és tágabban megfogalmazott kódexek. Tágabban meghatározott kódex például az, amely egy adott szektorba tartozó adatkezelők vagy adatfeldolgozók által folytatott adatkezelési műveletek mindegyikére kiterjed, az adatok gyűjtésétől kezdve a tároláson át egy esetleges adatvédelmi incidens esetén alkalmazandó eljárás rögzítéséig. Szűkebben meghatározott a tárgya egy olyan kódexnek például, amely csupán arra terjed ki, hogy a tagok az általuk tipikusan folytatott adatkezelések során hogyan biztosítják a tisztességesség és átláthatóság követelményét.

A GDPR egyébként konkrét „előnyöket" is rendel a magatartási kódexek alkalmazásához, mivel néhány rendelkezésében maga is rögzíti azt, hogy azt a felügyeleti hatóság figyelembe veszi egy esetleges eljárás során, illetve hogy az felhasználható az adott kötelezettségnek való megfelelés igazolása során. Ilyen rendelkezések a következők:

- A magatartási kódexekhez való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti általános kötelezettségeit (az adatkezelő kötelezettsége arra, hogy az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajtson végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik).[67]
- A magatartási kódexekhez való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatkezelő és az adatfeldolgozó teljesíti adatbiztonsággal összefüggő kötelezettségét (az adatkezelő és adatfeldolgozó azon kötelezettsége, hogy a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja).[68]
- Az adatkezelők, illetve adatfeldolgozók által végzett adatkezelési műveletek hatásainak értékelése – különösen az adatvédelmi hatásvizsgálatok – során is figyelembe kell venni, hogy a szóban forgó adatkezelők, illetve adatfeldolgozók teljesítik-e a 40. cikkben említett jóváhagyott magatartási kódexek előírásait.[69]
- Annak eldöntésekor, hogy szükség van-e közigazgatási bírság kiszabására, illetve a közigazgatási bírság összegének megállapításakor minden egyes esetben kellőképpen figyelembe kell venni többek között azt is, hogy az adatkezelő vagy az adatfeldolgozó tartotta-e magát a 40. cikk szerinti jóváhagyott magatartási kódexekhez.[70]

3.2. A magatartási kódex alapvető követelményei – „elfogadhatóság" feltételei

A Testület az általa elfogadott, iránymutatásban[71] meghatározta, hogy melyek azok a feltételek, amelyeknek teljesülnie kell, mielőtt az illetékes felügyeleti hatóság teljeskörűen értékel és megvizsgál egy kódexet. Ezek tehát tulajdonképpen a magatartási kódex „befogadhatóságának" a feltételei, amelynek a kérelmező általi önellenőrzésére létrehoztak egy ellenőrző listát[72] is:

67 GDPR 24. cikk.
68 GDPR 32. cikk.
69 GDPR 35. cikk (8) bekezdés.
70 GDPR 83. cikk (2) bekezdés j) pont.
71 Európai Adatvédelmi Testület 1/2019 iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről.
72 Uo. 3. Függelék.

- A benyújtott kódextervezetnek röviden és tömören be kell mutatnia a kódex célját, hatályát (például a tagok, adatkezelési tevékenység, érintettek, adattípusok, földrajzi hatály megjelölése), és azt, hogy milyen módon fogja megkönnyíteni, pontosítani az általános adatvédelmi rendelet hatékony alkalmazását.
- A kódexet az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek vagy egyéb szervezetek, vagyis a kódex felelősei nyújthatják be.[73] Ilyen szervezet lehet például kereskedelmi vagy érdekképviseleti szervezet, ágazati szervezetek, érdekcsoportok. A kérelem részeként a szervezetnek biztosítania kell arról a felügyeleti hatóságot, hogy az adott képviseleti szerv hatékony, és képes arra (például a tagjainak száma alapján, vagy a tapasztalatai alapján), hogy egy szektort érintő szabályrendszert kidolgozzon, és annak betartatására hatékony eszközöket hozzon létre.
- A kódextervezetnek pontosan meghatározott hatállyal kell rendelkeznie, amely alapján egyértelműen megállapítható, hogy mely adatkezelési műveletekre, illetve azzal kapcsolatban milyen kérdésekre terjed ki. Emellett nagyon fontos, hogy meghatározza azt is, hogy a kódex nemzeti vagy több tagállamot is érintő adatkezelési tevékenységekre vonatkozik, mivel ez kihatással van többek között a jóváhagyás folyamatára is.
- A kódex felelőseinek azt is indokolniuk kell a kérelem részeként, hogy mi alapján valószínűsítették, állapították meg a felügyeleti hatóság illetékességét. Ennek kiemelt jelentősége van a több tagállamot érintő kódex esetén.
- A kódexnek meg kell határoznia olyan mechanizmusokat, amelyek segítségével hatékonyan ellenőrizhető, hogy a kódex alkalmazását vállaló szervezetek betartják-e annak rendelkezéseit. Emellett meg kell határozni egy ellenőrző szervezetet is, amely olyan mechanizmusokat alkalmaz, melyek lehetővé teszik, hogy ellenőrizze a kódexnek való megfelelést, és megfelel az általános adatvédelmi rendelet 41. cikkében rögzített feltételeknek.[74]
- A kódex tervezetének tartalmaznia kell arra vonatkozó információkat, hogy a kérelmező milyen konzultációt folytatott annak létrehozását megelőzően. A GDPR ugyanis hangsúlyozza, hogy az érdekelt felekkel konzultálni kell kódex létrehozása, kiegészítése és módosítása során, így különösen – amennyiben megoldható – az érintettekkel is.
- Amennyiben a kódex olyan ágazatot érint, amelyre vonatkozóan a nemzeti jog sajátos rendelkezéseket tartalmaz, a kódex felelőseinek meg kell erősíteniük, hogy a tervezet megfelel az ilyen releváns nemzeti jogszabályoknak is.
- A kódex tervezetét olyan módon kell benyújtani, hogy az megfeleljen az illetékes felügyeleti hatóság nyelvi követelményeinek. A határon átnyúló kódexek esetén az illetékes felügyeleti hatóság nyelvén és angol nyelven is be kell nyújtani a tervezetet.

3.3. A magatartási kódex tartalmi követelményei

A GDPR viszonylag szűkszavúan határozza meg, hogy milyen tartalmi követelményei vannak egy magatartási kódexnek. Ez egyfelől előnyt jelent a kódexek felelőseinek, mivel rugalmasságot biztosít számukra, vagyis az adott szektor és a kódexhez csatlakozni kívánó szervek és az azok által folytatatott adatkezelési tevékenységekhez, illetve a kódex tervezett hatályához alakíthatják azt. A GDPR tehát csak általános jellegű, fő követelményeket határoz meg, amelyek értelmezéséhez, részletezéséhez segítséget nyújt a Testület iránymutatása.[75]

---

[73] GDPR 40. cikk (2) bekezdés.

[74] GDPR 40. cikk (4) bekezdés.

[75] Európai Adatvédelmi Testület 1/2019 iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről 6. pont (32–41. szakaszok).

A magatartási kódex alapvető célja, hogy pontosítsa a GDPR alkalmazását, például az alábbiakra vonatkozóan:[76]

- tisztességes és átlátható adatkezelés;
- az adatkezelők jogos érdekei meghatározott körülmények között;
- az adatgyűjtés;
- személyes adatok álnevesítése;
- a nyilvánosság és az érintettek tájékoztatása;
- az érintettek jogainak gyakorlása;
- a gyermekek tájékoztatása és védelme, valamint a szülői felügyelet gyakorlójától származó hozzájárulás kikérésének módja;
- a 24. és a 25. cikkben említett intézkedések és eljárások, valamint a 32. cikkben említett, az adatkezelés biztonságát szolgáló intézkedések;
- a felügyeleti hatóságok értesítése, valamint az érintettek tájékoztatása az adatvédelmi incidensekről;
- a személyes adatok harmadik országok vagy nemzetközi szervezetek részére történő továbbítása; vagy
- az adatkezelő és az érintettek között az adatkezeléssel kapcsolatban felmerülő vitás ügyek megoldására irányuló, nem bírósági útra tartozó eljárások és egyéb vitarendezési eljárások, az érintettek 77. és 79. cikk szerinti jogainak sérelme nélkül.

A kódex lényeges tartalmi eleme az, hogy megfeleljen az ágazat vagy a hatálya alá tartozó adatkezelési tevékenységek sajátosságainak, illetve megkönnyítse és pontosítsa az általános adatvédelmi rendelet alkalmazását. Ezek a követelmények megjelennek a III. 2. pontban kifejtett befogadhatósági feltételekben is, hiszen ezekre röviden és tömören a kérelem benyújtásakor is ki kell térni, például a kérelemhez fűzött kísérő dokumentumban, vagy akár a kérelem részeként. Ezek ugyanis olyan alapvető feltételek, tulajdonképpen a magatartási kódex fogalmi elemei, amelyeket a kódexnek összességében és részleteiben tükröznie kell, azonban a tervezet érdemi vizsgálatának is előfeltétele.

A magatartási kódex felelőseinek tehát be kell tudniuk mutatni, hogy miért szükséges létrehozni a kódexet, vagyis azt, hogy mely problémákat kívánja kezelni, illetve azt, hogy a kódexben lefektetett szabályok, gyakorlatok hatékonyak és előnyösek, nem csupán a tagok, hanem az érintettek számára is. Emellett a kérelmezőnek igazolnia kell azt is, hogy a kódex megkönnyíti a GDPR hatékony alkalmazását, és pontosítja az abban foglalt rendelkezéseket a kódex hatálya alá tartozó szervezetek vagy adatkezelési tevékenységek vonatkozásában. A kódexnek alkalmasnak kell lennie arra, hogy a tagjainál elősegítse a GDPR alkalmazását, és azt pontosítva konkrét szabályokat, jó gyakorlatokat, reális és teljesíthető normákat fektessen le, amelyek megfelelő színvonalat és belső konzisztenciát eredményeznek. A pontosságot segítheti például az, hogy az ágazatra jellemző terminológiát alkalmaz, és konkrét bevált gyakorlatokat mutat be és ír elő.

A kódexnek minden követelmény megvalósításakor figyelembe kell venni az azt alkalmazni kívánó tagok és adatkezelési tevékenységeik sajátosságait, hiszen az összes követelmény csak ennek függvényében értelmezhető: a kódex szükségessége, a GDPR hatékony alkalmazásának elősegítése és a GPDR alkalmazásának pontosítása során is figyelemmel kell lenni a sajátosságokra. Így például, amennyiben egy kódex az egészségügyi kutatási ágazat adatkezeléseire vonatkozik, akkor a kódex hatályának, céljának meghatározása során figyelemmel kell lenni ennek az ágazatnak a sajátosságaira. „A kódexnek tehát egy konkrét szektor vagy tevékenységi kör adatkezeléssel kapcsolatos kérdéseire kell fókuszálni, és megoldásokat kínálni a kódexet alkalmazó adatkezelők és adatfeldolgozók számára ezekkel a kérdésekkel kapcsolatban.”[77]

[76] GDPR 40. cikk (2) bekezdés.

[77] Péterfalvi Attila, Révész Balázs, Buzás Péter (szerk.): Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., Budapest, 2018, 262. o.

A kódex további elengedhetetlen tartalmi eleme az, hogy összhangban legyen a GDPR-ral, és elegendő és megfelelő garanciákat nyújtson.[78] Ennek a követelménynek a lényege az, hogy a kódex felelősei, figyelembe véve a kódex hatálya alá tartozó adatkezelési tevékenységek körülményeit és kockázatait is, alkalmas és hatékony biztosítékokat tartalmaz a kockázat enyhítése és az érintettek jogainak és szabadságainak biztosítása céljából. Ez alapján tehát egy magasabb kockázatú adatkezelés, például nagy mennyiségű egészségügyi adat kezelése esetén elvárható, hogy a kódex szigorúbb követelményeket támasszon az adatkezelőkkel és adatfeldolgozókkal szemben.

További alapvető elvárás egy kódexszel szemben az, hogy megfelelő mechanizmusokat írjon elő a kódexben rögzített, a tagok által vállalt kötelezettségek betartásának ellenőrzésére, és hatékony intézkedéseket vezessen be a megfelelés biztosítása érdekében. Ilyen mechanizmus lehet például a rendszeres ellenőrzési és jelentéstételi kötelezettségek, világos és átlátható panaszkezelési és vitarendezési eljárások, a kódex megsértése esetére szankciók és jogorvoslatok, valamint a kódex megsértésének bejelentésére szolgáló eljárások megalkotása, előírása. Emellett a kódexnek ki kell jelölnie ellenőrző szervezetet is,[79] amelyet az illetékes felügyeleti hatóság akkreditál.[80] Az ellenőrzési mechanizmusokkal szemben általános elvárás az, hogy azok hatékonyak, egyértelműek, érvényesíthetők, tesztelhetők és megvalósíthatók legyenek.

A felsorolt tartalmi követelményeknek való megfelelést a jóváhagyási eljárás során a kódex felelőseinek kell bemutatniuk és igazolniuk.

3.4. A magatartási kódex jóváhagyása

Ha az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesület vagy egyéb szervezet magatartási kódexet kíván kidolgozni, vagy a meglévő kódexet módosítani vagy kibővíteni, a tervezetet benyújtja az illetékes felügyeleti hatóságnak. A felügyeleti hatóság véleményt bocsát ki arról, hogy a tervezet összhangban van-e a GDPR-ral. Amennyiben azt állapítja meg, hogy a tervezet elegendő és megfelelő garanciákat nyújt, akkor jóváhagyja azt. Ezt követően az illetékes felügyeleti hatóság a jóváhagyott kódexet nyilvántartásba veszi, és közzéteszi.[81]

A GDPR megfogalmazása alapján tehát ahhoz, hogy egy magatartási kódex alkalmas legyen az alapvető céljának megvalósítására, vagyis arra, hogy az elszámoltathatóság alapelvének tükrében felhasználható legyen a GDPR-nak való megfelelés igazolása során, szükséges az illetékes felügyeleti hatóság jóváhagyása. Csak a jóváhagyott magatartási kódexhez való csatlakozás alapozza meg a GDPR releváns szakaszainak alkalmazását, így például azt, hogy a felügyeleti hatóság bírság kiszabása esetén figyelembe veszi ezt a tényt.

A jóváhagyás eljárásjogi kérdéseit nemzeti jogszabályok rendezik, azonban a Testület is lefektet néhány alapvető szabályt az iránymutatásában.[82] Ez alapján például a III. 2. pontban felsorolt és a Testület által kimunkált követelmények teljesítése feltétele annak, hogy az illetékes felügyeleti hatóság érdemben vizsgálja, értékelje a kódexet.

Az általános adatvédelmi rendelet alapján, a felügyeleti hatóság engedélyezési és tanácsadási hatáskörében eljárva a 40. cikk (5) bekezdésével összhangban véleményezi és jóváhagyja a magatartási

[78] GDPR 40. cikk (5) bekezdés.

[79] Ez a követelmény nem vonatkozik s közhatalmi szervek és közfeladatot ellátó egyéb szervek által végzett adatkezelésre vonatkozó kódexekre.

[80] Az ellenőrző szervezettel szemben támasztott követelmények, illetve az akkreditálás követelményeiről a III. 6. pont tartalmaz további információkat.

[81] GDPR 40. cikk (5)–(6) bekezdései.

[82] Európai Adatvédelmi Testület 1/2019 iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről 7. pont (42–57. szakaszok).

kódexek tervezetét.[83] A kérelmezőnek az illetékes felügyeleti hatósághoz kell benyújtania a tervezetet. Az illetékességnek a GDPR 55. cikkében lefektetett általános szabálya alapján a felügyeleti hatóság a saját tagállamának területén illetékes a GDPR alapján ráruházott feladatok végzésére és hatáskörök gyakorlására. Egy tagállamban alkalmazni kívánt magatartási kódex esetén általánosságban elmondható, hogy azt az adott tagállam felügyeleti hatóságának kell benyújtani jóváhagyásra.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) a 2018. évi XXXVIII. törvénnyel módosított, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján, a GDPR-ban meghatározott magatartási kódexek tervezetének jóváhagyása iránti kérelmek benyújtása esetén adatkezelési engedélyezési eljárást folytat le, amelynek ügyintézési határideje 180 nap. Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvényben meghatározottakon túl a kérelem tartalmazza a magatartási kódex (annak kiegészítése vagy módosítása) tervezetét. Több tagállamot érintő kódex jóváhagyása iránti eljárás során az egységességi mechanizmus alkalmazásának időtartamára a NAIH felfüggeszti eljárását. Ha a NAIH megállapítja, hogy a tervezet elegendő és megfelelő garanciákat biztosít, akkor határozatában jóváhagyja a magatartási kódexet (vagy annak kiegészítését, módosítását). Az adatkezelési engedélyezési eljárásért miniszteri rendeletben meghatározott mértékű igazgatási szolgáltatási díjat kell fizetni.[84]

3.5. Határon átnyúló kódexek

Előfordulhat, hogy egy magatartási kódex több tagállamot érintő adatkezelési tevékenységre vonatkozik, például amennyiben egy adott szektor európai érdekképviseleti szervezete dolgoz ki ilyen eszközt az összes tagállamra kiterjedő hatállyal.

Az ilyen határon átnyúló kódex esetén természetesen a tartalmi követelmények vonatkozásában is figyelembe kell venni azt a tényt, hogy a kódexet több tagállamban letelepedett, de egy ágazatba tartozó szervezetek fogják alkalmazni. Ennek a körülménynek tehát meg kell jelennie a követelmények kérelmező általi igazolása során is, így például a kódex hatályának, előnyeinek, az ellenőrzési mechanizmusok hatékonyságának, vagy a nemzeti jogszabályok figyelembevételének igazolása során is.

Amennyiben a kódex több tagállamot érintő adatkezelési tevékenységre vonatkozik, akkor a befogadhatósági követelmények részeként a kérelmezőnek indokolnia kell, hogy miért feltételezi az adott hatóság illetékességét. Ennek során több tényezőt figyelembe vehet, amely alapján meghatározható, hogy a kódex értékelése céljából melyik a legmegfelelőbb illetékes felügyeleti hatóság. Ilyen tényezők például:

- az a hely, ahol az adatkezelési tevékenység vagy ágazat a legjelentősebb;
- az a hely, ahol az érintettek száma a legnagyobb;
- a kódex felelősének székhelye;
- a javasolt ellenőrző szervezet székhelye;
- a felügyeleti hatóság konkrét területen kidolgozott kezdeményezései, iránymutatásai.[85]

[83] 58. cikk (3) bekezdés d).

[84] Infotv. 64/A-64/D. §; az igazgatási szolgáltatási díj az adatkezelési engedélyezési eljárás lefolytatásáért fizetendő igazgatási szolgáltatási díjról szóló, az igazságügyi miniszter 25/2018 (IX. 3.) IM rendelet alapján 530 000 forint.

[85] Európai Adatvédelmi Testület 1/2019 iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről 2. számú függelék.

Ilyen, határon átnyúló kódex jóváhagyására irányuló kérelem esetén a GDPR egységességi mechanizmus alkalmazását írja elő.[86] A Testület emellett a határon átnyúló kódexek jóváhagyásának GDPR-ban lefektetett szabályait kiegészítve, megalkotott egy együttműködési eljárást,[87] amelyet a Testületnek való benyújtást megelőzően alkalmaznak a felügyeleti hatóságok. Ennek során az illetékes felügyeleti hatóság mellett kijelölésre kerül egy vagy két közreműködő társhatóság, akik segítséget nyújtanak az illetékes hatóságnak a kódextervezet értékelésében. Amennyiben az illetékes hatóság a társhatóságokkal való egyeztetést követően úgy dönt, hogy jóvá kívánja hagyni a kódexet, akkor azt megküldi valamennyi felügyeleti hatóság számára véleményezésre. Ha ez az „informális" együttműködés lezárul, az illetékes hatóság a Testület elé terjeszti a jóváhagyásra irányuló döntéstervezetét, amely egységességi mechanizmus keretében véleményt bocsát ki arról, hogy az összhangban van-e a rendelettel, illetve hogy megfelelő garanciákat nyújt-e.[88]

Ha a Testület ezt megerősíti, akkor véleményét benyújtja a Bizottságnak. A Bizottság határozatban dönthet arról, hogy a hozzá benyújtott és jóváhagyott magatartási kódex (módosítás vagy kiegészítés) az Unió területén általános érvénnyel rendelkezik. A Bizottság által általános érvényűnek nyilvánított kódexek nyilvánosságát a Bizottság biztosítja. A Testület valamennyi jóváhagyott magatartási kódexet, módosítást és kiegészítést egy nyilvántartásban állítja össze, és megfelelő módon nyilvánosan elérhetővé teszi őket.[89]

Az általános érvénnyel rendelkező magatartási kódexet a GDPR hatálya alá nem tartozó adatkezelők vagy adatfeldolgozók is betarthatják annak érdekében, hogy megfelelő garanciákat nyújtsanak a személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása keretében. Az ilyen adatkezelők vagy adatfeldolgozók szerződéses vagy egyéb, jogilag kötelező erejű eszközök révén kötelező erejű és kikényszeríthető kötelezettségvállalást tesznek arra, hogy alkalmazzák a megfelelő garanciákat, ideértve az érintettek jogaira vonatkozókat is.[90]

3.6. A magatartási kódex ellenőrzése – az ellenőrző szervezetekre vonatkozó követelmények

Ahogy a III. 3. pontban is kifejtésre került, a magatartási kódexben rögzíteni kell olyan mechanizmusokat, amelyek hatékonyan biztosítják, hogy az alkalmazását vállaló szervezetek betartják az abban szereplő előírásokat. Ennek egyik elemeként a GDPR úgy rendelkezik, hogy a magatartási kódexnek való megfelelés ellenőrzését olyan szervezet végezheti, amely a kódex tárgya tekintetében megfelelő szakértelemmel rendelkezik, és amelyet az illetékes felügyeleti hatóság erre akkreditál. Ez a rendelkezés nem alkalmazandó a közhatalmi szervek és közfeladatot ellátó egyéb szervek által végzett adatkezelésre.[91]

Ahhoz tehát, hogy egy magatartási kódex megfeleljen a GDPR-ban előírtaknak, ki kell jelölnie egy ellenőrző szervezetet, amely a kódex rendelkezéseinek való megfelelést ellenőrzi. Az ilyen szervezetet – a közhatalmi vagy közfeladatot ellátó szervek adatkezelésére vonatkozó kódex kivételével – az illetékes felügyeleti hatóság akkreditálja.

A GDPR 41. cikke általános követelményeket fogalmaz meg az ilyen szervezetekkel szemben, és úgy rendelkezik, hogy a felügyeleti hatóságoknak közzé kell tennie az akkreditálással kapcsolatos szempontokat.[92] Ezáltal tulajdonképpen a felügyeleti hatóságok konkretizálják, részletezik a GDPR-

[86] GDPR 63. cikk.

[87] Részletszabályai az Európai Adatvédelmi Testület 1/2019 iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről 8. pontban (48–57. szakaszok), illetve 2. és 4. függelékben találhatók.

[88] GDPR 40. cikk (7) bekezdés és 64. cikk.

[89] GDPR 40. cikk (7)–(11) bekezdések.

[90] GDPR 46. cikk (2) bekezdés.

[91] GDPR 41. cikk (1) és (6) bekezdés.

[92] GDPR 42. cikk (3) bekezdés és 57. cikk (1) bekezdés p) pont.

ban előírt általános jellegű követelményeket. A hatóságok által kidolgozott szempontrendszer tervezetét be kell nyújtani a Testületnek, amely egységességi mechanizmus keretében véleményt bocsát ki róla.[93]

Az ellenőrző szervezet fő funkciója és feladata az, hogy a kódex valamely adatkezelő vagy adatfeldolgozó általi megsértése esetén megfelelő intézkedéseket hozzon, így például felfüggesztheti vagy kizárhatja az adatkezelőt vagy adatfeldolgozót a kódex alkalmazásából. Fontos megjegyezni, hogy az ellenőrző szervezetnek az ilyen intézkedésekről és azok indokairól tájékoztatnia kell az illetékes felügyeleti hatóságot.[94]

Az ellenőrző szervezetek akkreditálásának alapvető követelményei a következők:[95]

- Függetlenség

Az ellenőrző szervezet lehet külső vagy belső, aszerint, hogy része-e a kódex felelősét jelentő szervezetnek, vagy attól elkülönül. Mind a két modell megfelelhet a függetlenség előírásának, amennyiben megfelelően hozzák azokat létre. Belső ellenőrzési szervezetként kijelölhető például egy eseti belső bizottság, vagy egy különálló, független szervezeti egység a kódexet létrehozó szervezeten belül. Ilyen esetben a függetlenséget garantálni lehet például azáltal, hogy a belső szervezet a szervezet többi területeitől elkülönült személyzettel, irányítással és működéssel rendelkezik.

Az illetékes felügyeleti hatóság számára kielégítő bizonyítékot kell szolgáltatni arra nézve, hogy az ellenőrző szervezet független a kódex tagjaitól és a hatálya alá tartozó szakmától, ágazattól. A függetlenséget négy területen kell tudni igazolni.[96] Egyrészt az ellenőrző szervezet jogi formájának és felépítésének biztosítania kell azt, hogy döntései során befolyástól mentesen tud működni, és nem utasítható. Másodszor, az ellenőrző szervezetnek önálló gazdálkodásúnak, anyagilag stabilnak kell lennie, és rendelkeznie kell elegendő erőforrással a feladatai ellátásához. Harmadszor, az ellenőrző szervezetnek elegendő humánerőforrással és technikai erőforrással kell rendelkeznie, amely biztosítja, hogy a feladatait hatékonyan tudja ellátni. Végül fontos követelmény az is, hogy az ellenőrző szervezetnek elszámoltathatónak kell lennie, vagyis felelősségre vonhatónak a döntéseiért és intézkedéseiért.

- Összeférhetetlenség

Az akkreditálás során igazolni kell, hogy az ellenőrző szervezet feladatainak és kötelezettségeinek gyakorlása nem vezet összeférhetetlenséghez, vagyis azt, hogy tartózkodni fog minden olyan tevékenységtől, amely nem egyeztethető össze a feladataival és kötelezettségeivel. Szintén az összeférhetetlenség követelményének részeként kell igazolni azt, hogy az ellenőrző szervezet mentes a külső befolyástól, és nem kérhet vagy fogadhat el utasítást senkitől.

---

93 GDPR 41. cikk (3) bekezdés.

94 A GDPR 41. cikk (4) bekezdése írja elő ennek alkalmazását. A Testület a tananyag elkészítéséig egy felügyeleti hatóság által benyújtott szempontrendszerrel kapcsolatban alkotott véleményt: 9/2019. számú vélemény az Osztrák Adatvédelmi Hatóság által a magatartási kódexnek való megfelelést ellenőrző GDPR 41. cikk szerinti szervezet akkreditációjára vonatkozóan meghatározott szempontokról.

95 A GDPR 41. cikkében, és a Testület iránymutatásában rögzített alapvető követelményeket minden tagállam felügyeleti hatósága által elfogadott akkreditálásra vonatkozó szempontoknak tartalmazniuk kell. Ezeket a követelményeket az egyes felügyeleti hatóságok kiegészíthetik, vagy pontosíthatják, de az egységesség érdekében figyelemmel kell lenni a Testület iránymutatására. Erre hívják fel a figyelmet a Testület 9/2019. számú véleményének 4–5. szakaszai.

96 Európai Adatvédelmi Testület 9/2019. számú véleménye az Osztrák Adatvédelmi Hatóság által a magatartási kódexnek való megfelelést ellenőrző GDPR 41. cikk szerinti szervezet akkreditációjára vonatkozóan meghatározott szempontokról 12–24. szakaszai.

- Szakértelem

Igazolni kell, hogy az ellenőrző szervezet rendelkezik a feladatainak ellátásához szükséges szakértelemmel. A szakértelmet minden esetben a konkrét magatartási kódex tárgyához, tartalmához mérten kell megvizsgálni, hiszen más szakértelemre lehet szükség például egy az egészségügyi kutatási szektor által megalkotott kódex betartásának ellenőrzéséhez, mint a pénzügyi szektorba tartozó adatkezelők által alkalmazott kódex ellenőrzéséhez. Minden esetben fontos azonban, hogy az ellenőrző szervezet személyzete megfelelő tudással, tapasztalattal és képzettséggel rendelkezzen ahhoz, hogy a szabályok betartását ellenőrizze, és megfelelő intézkedésekről tudjon dönteni a betartás kikényszerítése érdekében.

- Megfelelő eljárások és struktúrák

Az ellenőrző szervezetnek megfelelő és kellően pontos és specifikus eljárásokat kell előírnia és alkalmaznia a kódex betartásának ellenőrzése céljából. Az akkreditálás során ezeket az eljárásokat, csakúgy, mint a szervezet struktúráját és működését részletesen be kell mutatni. A kidolgozott eljárásoknak alkalmasnak kell lenniük arra, hogy megfelelően értékelje a szervezet, hogy egy adatkezelő vagy adatfeldolgozó jogosult-e a kódexhez csatlakozni, illetve betartja-e a rendelkezéseit. Az eljárásoknak biztosítaniuk kell a magatartási kódex aktív és hatékony ellenőrzését, például előre be nem jelentett ellenőrzések, éves ellenőrzések, rendszeres jelentéstétel és kérdőívek használata révén.

- Átlátható panaszkezelés

A panaszok átlátható kezelésére alkalmazott eljárásrend kialakítása szintén feltétele egy ellenőrző szervezet akkreditálásának. Ennek nyilvánosan elérhetőnek kell lennie, és alkalmasnak kell lennie arra, hogy a panaszokat átlátható és pártatlan módon kezeljék. A panaszkezelés részeként biztosítani kell azt is, hogy az ellenőrző szervezet egy megalapozott panasz esetén megfelelő korrekciós intézkedést tudjon hozni (például figyelmeztetés, a tagság felfüggesztése vagy kizárás). Az eljárásrendnek ki kell térnie a határidőkre is, és arra is, hogy milyen módon tájékoztatja az ellenőrző szervezet a vizsgálat eredményéről a panaszost, a kódex tagjait és az illetékes felügyeleti hatóságot.

- Az illetékes felügyeleti hatósággal folytatott kommunikáció

Igazolni kell azt is, hogy az ellenőrző szerv javasolt formája, működése biztosítja, hogy a szervezet által hozott intézkedésekről tájékoztassa az illetékes és egyéb felügyeleti hatóságokat. Emellett rendelkeznie kell arról is, hogy az illetékes felügyeleti hatóságot milyen módon és gyakorisággal tájékoztatja a kódexben bekövetkezett módosításokról és az egyéb rendszeres ellenőrzések eredményéről, jelentésekről.

- Felülvizsgálati mechanizmusok

Biztosítottnak kell lennie annak is, hogy a kódexet a kódex felelősei bizonyos időközönként felülvizsgálják, így az releváns maradjon, és figyelembe vegye a jogszabályokban, azok értelmezésében, technológiában bekövetkezett és egyéb változásokat.

- Jogállás

Az akkreditálás során meg kell erősíteni, hogy az ellenőrző szervezet olyan jogi formával rendelkezik, amely lehetővé teszi, hogy az illetékes felügyeleti hatóság alkalmazza vele szemben a GDPR-ban

előírt szankciókat, például bírságolható legyen a 83. cikk (4) bekezdés c) pontja alapján. A Testület emellett pontosította, hogy csak olyan szervezet akkreditálható, amely rendelkezik tevékenységi hellyel az EGT-ben.[97]

Amennyiben egy szervezet nem, vagy már nem felel meg az akkreditációs feltételeknek, vagy ha az intézkedései megsértik a GDPR-t, akkor az illetékes felügyeleti hatóság visszavonja az akkreditációját.[98]

Magyarországon az Infotv. alapján a jóváhagyott magatartási kódexnek való megfelelés ellenőrzésére kijelölt szerv akkreditálása adatkezelési engedélyezési eljárás keretében történhet, amely a magatartási kódex jóváhagyásától elkülönülő eljárásban történik. A NAIH az ilyen ellenőrzési tevékenység engedélyezése iránti kérelem benyújtása esetén adatkezelési engedélyezési eljárást folytat le, amelynek ügyintézési határideje 180 nap. A kérelemnek tartalmaznia kell a GDPR-ban meghatározott, illetve a NAIH által közétett engedélyezési követelményekben meghatározott feltételek fennállásának igazolására szolgáló adatokat.[99] Az eljárása során a NAIH is irányadónak tartja a Testület által megfogalmazott iránymutatást, illetve az egységességi mechanizmusban ezzel kapcsolatban hozott vélemények tartalmát. Az adatkezelési engedélyezési eljárásért miniszteri rendeletben meghatározott mértékű igazgatási szolgáltatási díjat kell fizetni.[100]

97 A Testület 9/2019 véleménye, 52. szakasz.

98 GDPR 41. cikk (5) bekezdés.

99 Infotv. 64/A-64/D. §.

100 Az igazgatási szolgáltatási díj az adatkezelési engedélyezési eljárás lefolytatásáért fizetendő igazgatási szolgáltatási díjról szóló, az igazságügyi miniszter 25/2018 (IX. 3.) IM rendelet alapján 530 000 forint.

4. TANÚSÍTÁS ÉS AKKREDITÁCIÓ

Ahogy a tananyag bevezetőjében[101] is kifejtésre került, az adatvédelem területén alkalmazható tanúsítás a GDPR által a megfelelés igazolása céljából létrehozott egyik önkéntes eszköz. A fő célja az, hogy az adatkezelő vagy adatfeldolgozó felhasználhassa annak céljából, hogy igazolja, hogy az általa végzett adatkezelési művelet(ek) megfelel(nek) a GDPR előírásainak.

A tanúsítás GDPR-ban való megjelenése is annak a jele, hogy a korábbi, engedélyezési, bejelentési kötelezettségekre alapuló adatvédelmi mechanizmusokat, ex-ante jellegű kötelezettségeket (mint például korábban az Infotv. alapján az adatvédelmi nyilvántartásba történő bejelentés volt) a GDPR háttérbe szorítja, és inkább az ex-post, utólagos kikényszerítési, elszámoltathatósági mechanizmusokat részesíti előnyben.[102]

A GDPR hatálybalépését és alkalmazandóvá válását megelőzően is számos olyan tanúsítási rendszert és szempontrendszert hoztak létre, amelynek van adatvédelmi vonatkozása is. Ezek azonban nem hordozzák magukban a GDPR-ban foglalt előnyöket, következményeket (például azt, hogy a bírság kiszabás során a felügyeleti hatóságnak figyelembe kell vennie azt, ha egy adatkezelő vagy adatfeldolgozó releváns tanúsítvánnyal rendelkezik). Ezek a korábban létrehozott tanúsítások termékek, szolgáltatások, folyamatok és irányítási rendszerek tanúsítására szolgálnak, és részben szabványokra, részben jogszabályokra épülnek. Van olyan tanúsítás, mint például a német EuroPrise, amely egy szolgáltatással vagy termék által végzett adatkezelési műveletre irányulnak. A francia adatvédelmi hatóság által kínált jelölésnek többféle tárgya is lehet, például irányítási rendszer, termék, eljárás (adatvédelmi auditok lefolytatása) és akár képzések is.[103] Európában ezen kívül is számos, *részben vagy egészben adatvédelmi tárgyú tanúsítás létezik, például az egyesült királyságbeli* BS 10012 Personal Information Management System vagy a holland Myobi Privacy Seal. Ezek a jelenleg is létező tanúsítási rendszerek is nagy változatosságot mutatnak, például a tárgyukat, elterjedtségüket, földrajzi hatályukat, célzott szervezeteket (adatkezelő vagy adatfeldolgozó), szektorális vagy általános jellegüket is tekintve.

Az Európai Unión kívül is létezik számos tanúsítási rendszer, amely adatvédelemmel kapcsolatos, így például a japán Privacy Mark, vagy az Ázsiai és Csendes-óceáni Gazdasági Együttműködés (APEC, Asia-Pacific Economic Cooperation) által működtetett Cross-Border Privacy Rules (CBPR) System elnevezésű tanúsítás.

4.1. A tanúsítás lényege és alapfogalmai

A tagállamok, a felügyeleti hatóságok, a Testület, valamint a Bizottság – különösen uniós szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott

---

[101] I. pont.

[102] Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, Gabriela Bodea: Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679, Final Report, Európai Bizottság, 2019.

[103] European Union Agency For Network and Information Security: Recommendations on European Data Protection Certification. 2017. november.

adatkezelési műveletek megfelelnek a GDPR előírásainak. Figyelembe kell venni a mikro-, kis- és középvállalkozások sajátos igényeit.[104]

A tanúsítás fő előnye az, hogy segíti az adatkezelőket és adatfeldolgozókat a GDPR-nak való megfelelés igazolásában, illetve növeli a bizalmat az érintettek részéről azáltal, hogy adatkezelési tevékenységeiket is átláthatóbbá teszi.

A GDPR néhány konkrét kötelezettség esetében külön is rendelkezik arról, hogy a tanúsítás alkalmas a kötelezettségek adatkezelő vagy adatfeldolgozó általi teljesítésének igazolására. Ezek a következők:

- megfelelő technikai és szervezési intézkedéseket végrehajtása,[105]
- az adatfeldolgozó által megfelelő garanciák biztosítása.[106]

GDPR szerinti tanúsítást annak bizonyítására is létre lehet hozni, hogy a GDPR hatálya alá nem tartozó adatkezelők vagy adatfeldolgozók a 46. cikk (2) bekezdés f) pontjában foglalt feltételekkel összhangban megfelelő garanciákat nyújtsanak a személyes adatok harmadik országba történő továbbítása keretében. Ennek feltétele, hogy az ilyen adatkezelők vagy adatfeldolgozók szerződéses vagy egyéb, jogilag kötelező erejű eszközök révén kötelező erejű és kikényszeríthető kötelezettségvállalást tesznek arra, hogy alkalmazzák a megfelelő garanciákat, ideértve az érintettek jogaira vonatkozókat is.

A tanúsítási mechanizmus célja tehát az, hogy a GDPR-nak való megfelelés igazolásában segítse az adatkezelőket és adatfeldolgozókat. Ennek két gyakorlati következménye van: a tanúsítást egyrészt az elszámoltathatóság alapelvének fényében kell értelmezni; másrészt a GDPR-nak való megfelelés független a tanúsítás meglététől. A megfelelés általános követelmény a GDPR hatálya alá tartozó adatkezelést vagy adatfeldolgozást végző adatkezelők és adatfeldolgozók számára, a tanúsítás viszont egy önkéntes eszköz, amelynek segítségével egy adatkezelő vagy adatfeldolgozó igazolhatja, hogy a GDPR egy vagy több rendelkezésének milyen módon felel meg.[107]

A GDPR nem határozza meg, hogy mit jelent a tanúsítás, illetve az ezzel összefüggésben használt többi fogalmat sem definiálja, ezért azokat a GDPR rendelkezésein túl, a tanúsítással kapcsolatban nemzetközileg alkalmazott dokumentumok alapján kell értelmezni. A Nemzetközi Szabványügyi Testület (International Organization for Standardization, a továbbiakban: ISO) általános meghatározása alapján a tanúsítás olyan eljárás, amellyel egy független fél írásban igazolja, hogy egy termék, egy folyamat vagy egy szolgáltatás megfelel az előírt követelményeknek.[108] A tanúsítást úgy is szokták definiálni, hogy az egy harmadik fél általi megfelelőségértékelés.

A tanúsítás tehát meghatározott követelmények szerint folytatott megfelelőségértékelés, amelyet egy harmadik személy végez el és igazol. A követelmények szabványokból vagy jogszabályokból erednek, mint például a GDPR esetén, melynél a GDPR jelenti a normatív szabályrendszert, amely a követelmények értékelésének alapját képezi. A GDPR rendelkezéseit azonban pontosítani kell ahhoz, hogy megfeleljen a tanúsítás céljának. Egy sikeres tanúsítás eredménye a tanúsítvány, bélyegző vagy jelölés, amely igazolja, hogy az adott szervezet megfelelt a tanúsítási rendszerben, követelményekben pontosított és a szabványban vagy jogszabályban foglalt tartalmi és eljárási követelményeknek.[109]

A fentiek alapján, a GDPR szerinti tanúsítás egy adatkezelő vagy adatfeldolgozó által végzett adatkezelési művelet(ek) megfelelőségének harmadik, független fél általi igazolására utal.

---

104 GDPR (100) preambulumbekezdés; 42. cikk (1) bekezdés.

105 GDPR 24. cikk (1), (3) bekezdések, 25. cikk, és 32. cikk (1) és (3) bekezdések.

106 GDPR 28. cikk (1), (4) és (5) bekezdések.

107 Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, Gabriela Bodea: Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679, Final Report, Európai Bizottság, 2019, 19. o.

108 EN-ISO/IEC 17065/2012 szabvány.

109 European Union Agency For Network and Information Security: Recommendations on European Data Protection Certification. 2017. november.

Tanúsítási rendszer („certification scheme”) alatt olyan meghatározott termékekre, folyamatokra, szolgáltatásokra vonatkozó tanúsítási rendszert kell érteni, amelyekre ugyanazok az előírt követelmények, specifikus szabályok és eljárások vonatkoznak.[110] A tanúsítási rendszer tehát magában foglalja egy konkrét tanúsítás kibocsátásának szabályait, eljárását és menetét. A tanúsítási rendszer tulajdonosa lehet például egy tanúsító szervezet vagy egy felügyeleti hatóság is.

A tanúsítás alkalmazási területe vagy tárgya („scope of certification”) az alábbiak meghatározását jelenti:

- azon termékek, folyamatok, vagy szolgáltatások, amelyekre a tanúsítást megadják,
- az alkalmazható tanúsítási rendszer, és
- azon szabványok és más normatív dokumentumok, amelyek alapján úgy ítélik meg, hogy az adott termék, folyamat vagy szolgáltatás megfelelő.[111]

A GDPR szerinti tanúsítás tárgyának vagy alkalmazási területének meghatározása tehát arra ad választ, hogy a konkrét tanúsítás milyen típusú, jellegű adatkezelési művelet vagy műveletek összességének értékelésére, illetve megfelelőségének igazolására szolgálhat.

Tanúsítási követelmény („certification requirements”) a közvetlenül a termékre, folyamatra, szolgáltatásra vonatkozó, a tanúsítási rendszer által meghatározott szabványokban vagy más normatív dokumentumokban előírt követelményeket is tartalmazó követelményrendszer, amelyet az ügyfél teljesít a tanúsítás létrejöttének vagy fenntartásának feltételeként. Ez tehát utal egyrészt a normatív, tartalmi követelményekre és az eljárási követelményekre is. A tartalmi jellegű követelmények a GDPR szerinti tanúsítás esetében magából a GDPR-ból vezethetők le: az érintettek jogai, az adatbiztonság követelménye, a beépített és alapértelmezett adatvédelem elve például olyan normatív szabályok, amelyeket tanúsítási követelményekben pontosítani lehet. Emellett az eljárási követelmények szintén a tanúsítási rendszer részét képezik, és a tanúsítást igénylő szervezetnek ezeket is teljesítenie kell. Ilyen eljárási követelmények például azt pontosíthatják, hogy egy adatkezelő milyen feltételek mellett használhatja a megszerzett tanúsítványt, milyen időközönként van felülvizsgálat stb. Néhány eljárási kérdést maga a GDPR is tisztáz, például a tanúsítvány érvényességének időtartamát legfeljebb három évben határozza meg.[112]

A GDPR szerinti tanúsítási szempontok a tanúsítással összefüggésben általánosságban használt fogalmak közül a tanúsítási követelményekkel mutatnak legnagyobb hasonlóságot, hiszen a szempontok tartalmazzák a normatív jogszabályokban előírt kötelezettségek követelményként megfogalmazott megfelelőit, vagyis azon szempontokat, amely alapján elemezni lehet azt, hogy egy adatkezelési műveletet megfelel-e a GDPR releváns (a tanúsítás alkalmazási területe alapján meghatározott) rendelkezéseinek.

A GDPR nem határozza meg azt, hogy mit ért tanúsítási mechanizmus, tanúsítvány, bélyegző és jelölés alatt, és ezeket a kifejezéseket együttesen alkalmazza. A tanúsítvány egy megfelelőségi igazolás, míg a bélyegző és jelölés alkalmazása arra szolgál, hogy jelölje a tanúsítás sikeres elvégzését. A bélyegző vagy jelölés együttesen egy logóra vagy szimbólumra utalnak, amelynek a megjelenése (a tanúsítványon felül) azt jelöli, hogy a tanúsítás tárgyát független harmadik fél értékelte, és az megfelel a normatív dokumentumokban (például szabványokban, jogszabályokban) meghatározott követelményeknek. Ezeket a követelményeket a GDPR alkalmazásában a felügyeleti hatóság vagy a Testület által jóváhagyott szempontok tartalmazzák.[113]

A GDPR szerinti tanúsítványt tehát abban az esetben lehet kiállítani, ha egy akkreditált tanúsító

[110] EN-ISO/IEC 17065/2012 szabvány 3.9. pont.

[111] EN-ISO/IEC 17065/2012 szabvány 3.10. pont.

[112] European Union Agency For Network and Information Security: Recommendations on European Data Protection Certification. 2017. november.

[113] Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

szervezet, vagy felügyeleti hatóság általi, egy tanúsítási mechanizmus keretében végzett független megfelelőségértékelés alapján megállapítható, hogy az értékelés, vagyis a konkrét projekt tárgya a jóváhagyott tanúsítási szempontoknak megfelel.

4.2. A GDPR szerinti tanúsítás tárgya

Csakúgy, mint a magatartási kódex, a tanúsítás is rugalmasságot biztosít, hiszen az, hogy pontosan mit jelent, hogy egy tanúsítvány mit igazol, függ a konkrét tanúsítási mechanizmus, illetve az értékelés tárgyától is. Éppen ezért ezeknek a fogalmaknak az ismerete, illetve ezek pontos meghatározása kiemelkedően fontos, csak így érheti el a tanúsítás azt a célt, hogy segít a GDPR-nak való megfelelés igazolásában, és az érintettek felé érthető, egyértelmű és nem félreérthető üzenetet közvetít.

A Testület álláspontja szerint a GDPR tág alkalmazási kört határoz meg arra vonatkozóan, hogy mi tanúsítható. A fő feltétel az, hogy a tanúsítás segítse az adatkezelőket és adatfeldolgozókat abban, hogy igazolják, hogy egy adatkezelési művelet megfelel a GDPR előírásainak.[114]

A GDPR 43. cikk (1) bekezdés b) pontja az ISO 17065-ös szabványra utal, amely olyan tanúsító szervezetek akkreditációjáról szól, amelyek termékek, folyamatok és szolgáltatások megfelelőségértékelését végzik. Egy adatkezelési művelet vagy műveletek összessége az ISO 17065-ös szabvány szerinti terméket, folyamatot vagy szolgáltatást eredményezhet, vagyis ezek képezhetik a tanúsítás tárgyát. Például munkavállalói adatok bérek kifizetése céljából való kezelése a GDPR értelmében adatkezelési műveletnek tekinthető, és az említett szabvány szerinti terméket, folyamatot vagy szolgáltatást eredményezhet.[115]

A GDPR rendelkezései alapján a tanúsítás tárgya tehát az adatkezelő által végrehajtott adatkezelési művelet vagy műveletek összessége lehet. Azt azonban nem határozza meg a GDPR, hogy egy adatkezelési művelettel kapcsolatban mire terjedhet ki a tanúsítás. Elképzelhető, hogy az adott művelettel kapcsolatban csak egy konkrét GDPR szerinti kötelezettség teljesítését igazolja egy tanúsítvány, de az is, hogy akár az adott adatkezelési műveletre vonatkozóan az összes GDPR-beli kötelezettség teljesítését.[116]

A tanúsítás alkalmazási területével kapcsolatban a GDPR további rendelkezései is adnak támpontot: tanúsítványt adatkezelő vagy adatfeldolgozó részére lehet kiállítani, amelyből az következik, hogy adatvédelmi tisztviselők részére nem lehet, vagyis a GDPR szerinti tanúsítás tárgya nem lehet egy személy tisztviselőként tanúsítása.[117]

Meg kell különböztetni a tanúsítás alkalmazási területétől, tárgyától („scope of certification") az értékelés tárgyát („target of evaluation"), amely azt határozza meg, hogy egy tanúsítási mechanizmus alapján történő konkrét tanúsítási eljárásnak (projektnek) mi a tárgya. Egy tanúsítási mechanizmusnak lehet általános alkalmazási területe, tárgya, de lehet egy specifikus területre, adatkezelési típusra vonatkozó (például egészségügyi adatok kezelése) is. Ezáltal elképzelhető, hogy a mechanizmus tárgya annyira specifikus, hogy az értékelés tárgyának meghatározása nagyon egyszerű. Ha például egy tanúsítási mechanizmus tárgya a biztonságos bejelentkezés egy online felületre, akkor egy bank által üzemeltetett internetbankra vonatkozó tanúsítás esetén az ehhez a felülethez tartozó bejelentkezési felület lehet a konkrét „projekt" tárgya, vagyis az értékelés tárgya.

---

114 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

115 Uo.

116 Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, Gabriela Bodea: Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679, Final Report, Európai Bizottság, 2019, 20. o.

117 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

4.3. Tanúsítási szempontok

A GDPR szerinti tanúsítvány, bélyegző vagy jelölés kibocsátására akkor kerülhet sor, ha az akkreditált tanúsító szervezet vagy a felügyeleti hatóság független értékelést követően megállapítja, hogy a tanúsítási szempontok megfelelően teljesülnek az adott projekt tárgyát képező adatkezelési műveletre vonatkozóan.[118]

A tanúsítási mechanizmusnak a szempontokon kívül ki kell térnie azon követelményekre is, amelyek meghatározzák, hogy kinek, milyen mértékben és részletességgel kell az értékelést egy konkrét értékelési tárgyra, adatkezelési műveletre vonatkozó tanúsítási projekt során elvégeznie. A tanúsítási szempontok azokat a követelményeket jelentik, amelyek alapján az értékelési tárgyban megjelölt adatkezelési művelet megfelelőségét értékelni kell.

„A tanúsítási szempontoknak levezethetőnek kell lenniük a GDPR alapelveiből és szabályaiból, és segítséget kell nyújtaniuk abban, hogy a megfelelést igazolják. A szempontokat úgy kell meghatározni, hogy azok érthetők, egyértelműek és a gyakorlatban alkalmazhatók legyenek."[119]

Az általános adatvédelmi rendelet nem pontosítja, hogy ki alkothat tanúsítási szempontokat, illetve mechanizmust, csupán arról rendelkezik, hogy azokat a felügyeleti hatóságnak – a Testület véleményének kikérése mellett – jóvá kell hagynia.[120] Tanúsítási szempontokat tehát kidolgozhatnak, és a felügyeleti hatóságnak jóváhagyásra benyújthatnak például tanúsítási szervezetek, szabványügyi testületek, iparági szervezetek.[121] A GDPR azt a lehetőséget sem zárja ki, hogy felügyeleti hatóságok dolgozzanak ki tanúsítási szempontokat.

4.3.1. Tanúsítási szempontok kidolgozása

Egy adatkezelési művelet értékelése során három fő alapvető körülményt kell megvizsgálni: a személyes adatok (a GDPR tárgyi hatálya); a személyes adatok kezelése során alkalmazott technikai rendszerek, intézkedések (az infrastruktúra, például hardver és szoftver); és az adatkezeléshez kapcsolódó eljárások és folyamatok. Mind a három említett alapvető elemet figyelembe kell venni a tanúsítási eljárások és szempontok kidolgozása során.[122]

A tanúsítási szempontokat olyan módon kell megalkotni, hogy az alapján megfelelően megvizsgálható és elemezhető legyen az, hogy a GDPR-ban előírt egy vagy több kötelezettségnek (attól függően, hogy mi a tanúsítás tárgya, alkalmazási területe) megfelel-e a kérelmező az értékelés tárgyát képző adatkezelési tevékenységre vonatkoztatva. A szempontoknak az absztrakt normatív előírásokat – jelen esetben a GDPR előírásait – ellenőrizhető, konkrét követelményekké kell formázniuk.

---

118 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

119 Péterfalvi Attila, Révész Balázs, Buzás Péter (szerk.): Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., Budapest, 2018, 271. o.

120 GDPR 42. cikk (5) bekezdés és 64. cikk (1) bekezdés c) pont.

121 Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, Gabriela Bodea: Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679, Final Report, Európai Bizottság, 2019, 22–23. o.

122 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

A tanúsítási szempontrendszerrel kapcsolatban az alábbi általános követelményeket fogalmazta meg a Testület:[123]

- legyen egységes és ellenőrizhető;
- auditálható legyen annak érdekében, hogy megkönnyítse az adatkezelési művelet megfelelőségének értékelését;
- legyen releváns a célközönség számára;
- vegyen figyelembe más szabványokat (például ISO vagy nemzeti szabvány), és ha szükséges, legyen átjárhatóság azokkal; és
- legyen rugalmas, hogy különböző méretű és típusú szervezetek számára is alkalmas legyen, mint például kis- és középvállalkozások számára, illetve figyelembe tudja venni a kockázatalapú megközelítést.

A fentieken túlmenően vannak olyan formális követelmények, amelyeknek egy konkrét tanúsítási mechanizmusra vonatkozó meghatározása segíthet a tanúsítási szempontok kidolgozása során, és amelyek megkönnyíthetik az értékelést végző szakértők munkáját is.[124]

- A releváns előírások, szabályozások azonosítása
  Az adatvédelmi tanúsítás esetében ez tipikusan a GDPR lesz, de egyéb előírásokat is beépíthetnek, mint például ISO-szabványokat.
- Az előírások csoportosítása
  A szempontok követhetik a GDPR felépítését, vagy csoportosíthatják azokat témák vagy folyamatok mentén, amelyek koncepcionálisan összefüggenek. Például elképzelhető, hogy az „adatbiztonsági megfontolások", vagy „érintetti jogok gyakorlása" ilyen kategóriaként csoportosít több követelményt.
- Az előírások és azok alóli kivételek priorizálása
  A GDPR rendelkezései között van bizonyos sorrendiség, a kötelezettségek alóli kivételek is meg vannak határozva számos esetben. Ez alapján tanácsos úgy felépíteni a kritériumokat, hogy ezt tükrözze (például ha az értékelés tárgyát képező adatkezelési művelet nem érint különleges személyes adatokat, akkor minden ehhez kapcsolódó követelmény irreleváns lesz).
- A hivatkozások és követelmények közötti kapcsolat nyomonkövethetősége
  A szempontoknak kifejezetten tartalmazniuk kell hivatkozást a követelmény és annak forrása között. Ez segítséget nyújt a felügyeleti hatóságok számára, hogy megítéljék, minden releváns követelmény szerepel-e, illetve hozzájárul az átláthatósághoz is.
- A szempontok magyarázata
  Mivel a szempontrendszer nem feltétlenül magától értetődő, ezért fontos, hogy a különböző követelmények mellett magyarázat is szerepeljen.
- Pontos és félreérthetetlen
- Átfogó, de tömör
  Lefedi az összes releváns rendelkezést a GDPR-ból, de az értékelés rendszere kezelhető és jól rendszerezett marad, nincsenek felesleges részek.
- Közvetlen és eredményorientált
  Közvetlenül a releváns GDPR-előírásokra reflektálnak, és elegendő információt nyújtanak ahhoz, hogy megalapozott értékítéletet lehessen hozni, amely alapján az értékelés megszületik.
- Mérhető és következetesen alkalmazott
  Lehetővé teszi az értékelők között a konzisztens összehasonlítást.
- Érthető

[123] Uo.

[124] Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, Gabriela Bodea: Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679, Final Report, Európai Bizottság, 2019, 83–84.o.

- Gyakorlatias
- A kétségekkel, bizonytalanságokkal kapcsolatban világos
  Célja, hogy feltárja a különbségeket a lehetséges eredmények között, amelyeket a különböző értékelők a szempontok különböző alkalmazása során kaphatnak.

A megfelelőségértékeléshez szükséges meghatározni az értékelés módszertanát, vagyis az alkalmazott értékelési módszereket, hiszen például az, hogy milyen módon kerül sor a szükséges információ beszerzésére, kihatással van a tanúsítás súlyára, jelentőségére.

A tanúsítás egészét – így különösen azt, hogy mi az értékelés tárgya és mik az alkalmazott módszerek – részletesen dokumentálni kell, ez garantálja ugyanis a tanúsítási mechanizmus szerinti értékelési folyamatok átláthatóságát. A dokumentáció megléte azért is fontos, hogy ha esetlegesen a felügyeleti hatóság vizsgálata során dönteni kíván arról, hogy milyen mértékben veszi figyelembe a tanúsítást, akkor rendelkezésre álljon egy mindenre kiterjedő dokumentáció, amelyet az adatkezelő vagy adatfeldolgozó be tud mutatni. A megfelelő dokumentálás szükségessége egyébként az elszámoltathatóság elvéből is következik. A tanúsítás GDPR-ban lefektetett szerepéből következően kiemelten fontos, hogy a tanúsítás kibocsátása átlátható módon történjen: szükséges az alátámasztó dokumentumok megléte, így például jelentések, amelyek leírják, hogy milyen módon történt az értékelés, és mi indokolta a tanúsítvány kibocsátását. Az egyes – tanúsítvány kibocsátására, megújítására, vagy visszavonására vonatkozó – döntéseknek tartalmaznia kell az indokokat, bizonyítékokat, amelyek a szempontok alkalmazása alapján keletkeztek, illetve a következtetéseket, értékeléseket, egyéb tényeket, amelyeket a tanúsítás során gyűjtött a tanúsító szervezet.[125]

Nemcsak a tanúsítás, hanem a tanúsítás eredményének dokumentálása és közlése is kiemelt fontossággal bír. Az olyan tanúsítási mechanizmusok esetén, amelyeknek célközönsége az érintettek, könnyen hozzáférhető, közérthető és hasznos információkat kell rendelkezésre bocsátani.

4.3.2. Tanúsítási szempontok jóváhagyása

A tanúsítási szempontok szerves részét képezik a tanúsítási mechanizmusnak, ezért a GDPR úgy rendelkezik, hogy az akkor jelentheti egy tanúsítvány kibocsátásának alapját, ha az illetékes felügyeleti hatóság jóváhagyta.[126] A jóváhagyás célja, hogy a szempontok megfelelően tükrözzék a GDPR-ban rögzített adatvédelmi követelményeket, és hogy hozzájáruljanak a GDPR következetes alkalmazásához. A szempontok jóváhagyására akkor kerülhet sor, ha a tanúsítási mechanizmus alkalmas arra, hogy az adatkezelők és adatfeldolgozók igazolják a GDPR-nak való megfelelést.[127]

A tanúsítási szempontok jóváhagyására a tanúsító szervezet akkreditációját megelőzően, vagy azzal egyidejűleg kell hogy sor kerüljön.[128] Egy tanúsító szervezet egy adott tagállamban csak az adott tagállam felügyeleti hatósága által jóváhagyott tanúsítási szempontok alapján bocsáthat ki tanúsítványt. Ez azt jelenti, hogy a tanúsítási szempontokat azon tagállam felügyeleti hatóságának kell jóváhagynia, amelynek területén a tanúsító szervezet tanúsítványt kíván kibocsátani, és ahol az

[125] Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

[126] GDPR 42. cikk (5) bekezdés.

[127] Uo.

[128] Ennek indokait lásd részletesen a IV.3.2. pontban.

akkreditációja történik. A tanúsító szervezet ehelyett dönthet úgy is, hogy a Testület által jóváhagyott szempontok alapján kíván tanúsítványt kiállítani, melynek eredményeként közös tanúsítvány, az európai adatvédelmi bélyegző állítható ki.[129] Az ilyen, Testület által jóváhagyott szempontok alapján minden tagállamban lehet tanúsítványt kibocsátani.

A tanúsítási szempontok jóváhagyására irányuló döntés tervezetét az illetékes felügyeleti hatóság benyújtja a Testületnek, amely erről véleményt bocsát ki.[130]

Magyarországon az Infotv. alapján a tanúsítási szempontok jóváhagyása adatkezelési engedélyezési eljárásban történik, amelynek során a kérelem részeként be kell nyújtani a NAIH részére a tanúsítási mechanizmus általános leírását és a tanúsítási szempontok tervezetét. Az ügyintézési határidő 180 nap, amelyet az egységességi mechanizmus alkalmazásának időtartamára a NAIH felfüggeszt. Az adatkezelési engedélyezési eljárásért miniszteri rendeletben meghatározott mértékű igazgatási szolgáltatási díjat kell fizetni.[131] A NAIH tehát ilyen engedélyezési eljárás keretében hagyhat jóvá tanúsítási szempontokat, amelyet azonban a döntéstervezet Testületnek való megküldésekor felfüggeszt. Tekintettel a GDPR 64. cikk (1) bekezdés c) pontjára, erre minden alkalommal sor kerül, amikor tanúsítási szempontokat kíván jóváhagyni.

4.3.3. Az európai adatvédelmi bélyegző

A Testület által jóváhagyott tanúsítási szempontok eredményeként közös tanúsítvány, az európai adatvédelmi bélyegző állítható ki.[132]

Amennyiben egy szervezet európai adatvédelmi bélyegzőt kíván létrehozni, akkor az ennek alapját képező szempontrendszert be kell nyújtania az illetékes felügyeleti hatóságnak, és jeleznie kell, hogy az a szándéka, hogy a benyújtott szempontok alapján az összes tagállamban lehessen tanúsítványt kiállítani. A felügyeleti hatóság illetékességét megalapozhatja például a tanúsítási rendszer, mechanizmus kidolgozójának vagy a tanúsító szervezetnek a székhelye. Amennyiben az illetékes felügyeleti hatóság úgy ítéli meg, hogy a szempontok jóváhagyhatók, akkor benyújtja azt a Testületnek.[133]

Az európai adatvédelmi bélyegző esetében a szempontokat tehát a Testületnek kell jóváhagynia, és biztosítania kell azt, hogy minden tagállamban alkalmazható legyen, figyelembe véve a nemzeti jogi és szektor specifikus előírásokat. Az ilyen szempontoknak tehát a nemzeti előírásoknak megfelelően alakíthatóknak kell lenniük, a tanúsítási megállapodásoknak tükrözniük kell az összeurópai követelményeket, és létre kell hozni olyan eljárásokat, amelyek garantálják, hogy a nemzeti sajátosságokat figyelembe veszik, és a bélyegző ténylegesen segít a GDPR-nak való megfelelés igazolásában. Emellett arra is ki kell térnie, hogy milyen nyelven tájékoztatja az érintett felügyeleti hatóságokat a GDPR 43. cikk (1) és (5) bekezdésében előírt információkról.

Ahogy az a fentiekből is következik, az európai adatvédelmi bélyegző fő előnye, hogy az minden tagállamban kiállítható, így az Európa-szerte egységesen hozzáadott értéket képvisel az adatkezelők és adatfeldolgozók számára a GDPR-nak való megfelelés igazolása során. Emellett például egy olyan adatkezelő vagy adatfeldolgozó számára, amely több tagállamban is rendelkezik tevékenységi hellyel, praktikusabb lehet, hiszen ezáltal a tanúsítás folyamata leegyszerűsödhet: a különböző tagállamokban

[129] Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

[130] GDPR 64. cikk (1) bekezdés c).

[131] Infotv. 64/A-64/C. §. Az igazgatási szolgáltatási díj az adatkezelési engedélyezési eljárás lefolytatásáért fizetendő igazgatási szolgáltatási díjról szóló, az igazságügyi miniszter 25/2018 (IX. 3.) IM rendelet alapján 684 000 forint.

[132] GDPR 42. cikk (5) bekezdés.

[133] Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

található tevékenységi hely által folytatott adatkezelési műveletet ugyanazon szempontok alapján értékelik.

4.4. A tanúsítás folyamata és szereplői

A tanúsítványt akkreditált tanúsító szervezetek vagy az illetékes felügyeleti hatóságok állítják ki az illetékes felügyeleti hatóság által, vagy a Testület által jóváhagyott szempontok alapján.[134]

A GDPR fenti rendelkezése alapján tehát két szereplő állíthat ki tanúsítványt: a felügyeleti hatóságok vagy az akkreditált tanúsító szervezetek. A tanúsítvány kiállításának alapját pedig a jóváhagyott tanúsítási szempontok jelentik, vagyis ezeket alkalmazva kerülhet sor annak értékelésére, hogy egy adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési művelet („az értékelés tárgya") megfelel-e GDPR előírásainak. Amennyiben a szempontokat a Testület hagyta jóvá, az alapján bármely tagállamban európai adatvédelmi bélyegző állítható ki.

4.4.1. A felügyeleti hatóságok szerepe

A felügyeleti hatóságok szerepe a tanúsításban sokszínű. Kiállíthatnak maguk is tanúsítványokat, de a GDPR ezt nem teszi kötelező feladattá. A GDPR rendelkezései alapján azonban számos különböző modell lehetséges, amelyek közül a felügyeleti hatóságok egyet vagy akár többet is választhatnak:

- a hatóság saját tanúsítási rendszere alapján állít ki tanúsítványt;
- a hatóság saját tanúsítási rendszere alapján állít ki tanúsítványt, de a megfelelőségértékelést vagy egy részét harmadik felekre delegálja;
- a hatóság maga dolgoz ki egy tanúsítási rendszert, de a tanúsítás lefolytatását tanúsító szervezetekre bízza, amelyek a tanúsítványt is kiállítják;
- a hatóság ösztönzi a piaci szereplőket tanúsítási rendszerek kidolgozására.[135]

Amennyiben egy felügyeleti hatóság úgy dönt, hogy maga is végez tanúsítást, akkor ügyelnie kell rá, hogy átláthatóan gyakorolja hatásköreit. Különös figyelmet kell fordítania a tanúsítással kapcsolatos, illetve a vizsgálati és korrekciós hatáskörök elválasztására annak érdekében, hogy elkerülje az esetleges összeférhetetlenséget. Emellett a felügyeleti hatóságnak ilyen esetben meg kell határoznia a tartalmi és eljárási követelményeket. Szintén ajánlott a Testület álláspontja szerint, hogy a tanúsítást végző felügyeleti hatóságok kövessék az akkreditációról szóló iránymutatásban foglalt követelményeket és szempontokat.[136]

---

134 GDPR 42. cikk (5) bekezdés.

135 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

136 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

Vannak olyan, a tanúsítással összefüggő feladatai is a felügyeleti hatóságoknak, amelyeknek minden esetben, függetlenül attól, hogy ők maguk végeznek-e tanúsítást, eleget kell tenniük:

- értékeli és jóváhagyja a tanúsítási szempontokat, és a jóváhagyásra vonatkozó döntéstervezetet készít;[137]
- az így elkészített döntéstervezetet közli a Testülettel, és figyelembe veszi annak véleményét;[138]
- jóváhagyja a tanúsítási szempontokat, mielőtt akkreditációra és tanúsításra sor kerülhet;[139]
- közzéteszi a jóváhagyott tanúsítási szempontokat, és továbbítja azokat a Testület részére;[140]
- európai adatvédelmi bélyegzőt eredményező tanúsítási mechanizmus esetén ellátja az illetékes felügyeleti hatóság szerepét;[141]
- visszavonja a tanúsítványt, vagy utasítja a tanúsító szervezetet a kiadott tanúsítvány visszavonására, vagy utasítja a tanúsító szervezetet, hogy ne adja ki a tanúsítványt, ha annak feltételei (tanúsítási eljárás vagy a tanúsítási szempontok) nem vagy már nem teljesülnek.[142]

A NAIH-nak a tanúsítási szempontokkal kapcsolatos eljárására az Infotv. 64/A–64/D. §-ai alkalmazandók, melynek részletei megtalálhatók a IV.2.2. pontban.

Az Infotv. úgy rendelkezik, hogy a NAIH folytathat a GDPR-ban meghatározott tanúsítást is, az adatkezelő vagy adatfeldolgozó kezdeményezésére, a velük kötött megállapodás alapján. A NAIH-nak közzé kell tennie a megállapodás megkötésének feltételeit, a tanúsításért nyújtandó ellenszolgáltatást, a tanúsítás lefolytatásának menetét és a tanúsítási szempontokat. Ha a NAIH tanúsítványt vagy európai adatvédelmi bélyegzőt állít ki, közzéteszi a használatára jogosult adatkezelő vagy adatfeldolgozó megnevezését, és azon adatkezelési műveleteket, amelyekre a tanúsítvány vagy bélyegző kiterjed.[143] A NAIH-nak tehát a jogszabály alapján van lehetősége arra, hogy éljen a GDPR-ban is megfogalmazott lehetőséggel, és maga állítson ki tanúsítványt, akár a saját maga, akár más szervezet által kidolgozott szempontrendszer alapján.

A felügyeleti hatóságnak a tanúsítvány kibocsátását követően is vannak feladatai, így például, amennyiben egy akkreditált tanúsító szervezet tanúsítványt állít ki vagy újít meg, arról tájékoztatnia kell az illetékes felügyeleti hatóságot, amelynek során közölnie kell a tanúsítvány megadásának vagy visszavonásának okait is.[144] Bár ez a rendelkezés közvetlenül nem a hatóságok számára ír elő kötelezettséget, hanem a tanúsító szervezetnek, a felügyeleti hatóság szempontjából is kiemelt jelentősége van. A tanúsító szervezet ezen kötelezettségének következetes betartása teszi ugyanis lehetővé a felügyeleti hatóság számára azt, hogy gyakorolja az 58. cikk (2) bekezdés h) pontja szerinti hatáskörét, és visszavonjon egy tanúsítványt, vagy utasítsa a tanúsító szervezetet a kiadott tanúsítvány visszavonására, vagy arra, hogy ne adja ki a tanúsítványt, ha a tanúsítás feltételei nem vagy már nem teljesülnek. A felügyeleti hatóságok számára így biztosított hatáskör garantálja azt, hogy az akkreditált tanúsító szervezetek által kiállított tanúsítványok, jelölések, bélyegzők felett is gyakoroljanak ellenőrzést a hatóságok, és átláthatóvá, kikényszeríthetővé tegye a tanúsítványok alkalmazását.

Amint látható, a felügyeleti hatóságok számára a GDPR számos feladatot és hatáskört határoz meg a tanúsítással kapcsolatban, illetve olyan feladatokat is meghatároz, amelyeknek gyakorlása számukra nem kötelező. A felügyeleti hatóságoknak ezek alapján lehetőségük van arra, hogy általánosságban véve az adatvédelmi tanúsítással kapcsolatban meghatározó szerepük legyen, és ezáltal biztosítsák azt, hogy azok ténylegesen és hatékonyan járuljanak hozzá a GDPR-nak való megfelelés ösztönzéséhez.

137 GDPR 58. cikk (3) bekezdés f) és 42. cikk (5) bekezdés.
138 GDPR 64. cikk (1) bekezdés c), 64. cikk (7) bekezdés és 70. cikk (1) bekezdés (t).
139 GDPR 42. cikk (5) bekezdés és 43. cikk (2) bekezdés b).
140 GDPR 43. cikk (6) bekezdés.
141 GDPR 42. cikk (5) bekezdés és 70. cikk (1) bekezdés o).
142 GDPR 58. cikk (2) bekezdés h).
143 Infotv. 69. §.
144 GDPR 43. cikk (1) és (5) bekezdés.

4.4.2. A tanúsító szervezet

Ahogy már korábban is kifejtésre került, az általános adatvédelmi rendelet alapján tanúsítványt a felügyeleti hatóságokon kívül akkreditált tanúsító szervezetek is kiállíthatnak. A tanúsító szervezet („certification body") egy tanúsítási rendszereket működtető, harmadik félként működő megfelelőségértékelő szervezetet jelent.[145]

A tanúsítvány kiállításának alapját minden esetben a felügyeleti hatóság vagy a Testület által jóváhagyott szempontok jelentik. A tanúsítvány kiállítását és megújítását olyan tanúsító szervezet végzi, amely az adatvédelem terén megfelelő szakértelemmel rendelkezik.[146]

A GDPR alapján a tanúsító szervezet szerepe tehát az, hogy kiállítja, rendszeres időközönként felülvizsgálja, megújítja és visszavonja a tanúsítványt.[147] Ehhez az szükséges, hogy a tanúsító szervezet, vagy a rendszertulajdonos („scheme owner") létrehozzon tanúsítási eljárásokat, és ennek részeként meghatározzon eljárásrendet a tanúsítás ellenőrzésére, nyomon követésére, rendszeres felülvizsgálatára, panaszkezelésre és a visszavonásra, emellett az akkreditáció során meg kell határoznia a tanúsítási szempontokat és azon szabályokat, eljárásokat, mely alapján sor kerül a tanúsítvány, bélyegző vagy jelölés kiállítására.[148]

A fentiek már röviden utalnak arra, hogy milyen feltételei vannak annak, hogy egy tanúsítási szervezetet egy GDPR szerinti adatvédelmi tanúsítványt, jelölést vagy bélyegzőt állítson ki. Mindenekelőtt kiemelt szerepe van a megfelelő szakértelemnek, de ezt kiegészíti számos olyan követelmény, amely garantálja, hogy egy szervezet ténylegesen alkalmas a tanúsítvány kiállítására. Azt a folyamatot, amely során ezt megvizsgálja az arra rendelt szerv, és a végén megállapítja az adott szervezet, akkreditálásnak nevezik. Az ezzel kapcsolatos részletes tudnivalókat a következő (IV.4.) pont tartalmazza.

Mielőtt megállapításra kerül, hogy egy tanúsító szervezet egy konkrét tanúsítványt kiállíthat, szükséges az alkalmazni kívánt szempontrendszer és a tanúsítási mechanizmus megléte. Ennek oka, hogy csak konkrétan ezekre vonatkoztatva lehet azt megvizsgálni és megállapítani, hogy egy adott szervezet alkalmas-e a tanúsítás lefolytatására, például rendelkezik-e megfelelő szakértelemmel. Amennyiben például a tanúsítás tárgya, alkalmazási területe a korábban példaként említett biztonságos bejelentkezés, akkor a tanúsító szervezetnek rendelkeznie kell olyan szakértelemmel, illetve meg kell határoznia olyan konkrét eljárásokat, amelyeknek segítségével egy adott adatkezelő vagy adatfeldolgozó által működtetett bejelentkezési felületet meg tud vizsgálni, és annak megfelelőségét vagy adott esetben hiányosságait megállapítani.

A tanúsító szervezeteknek a GDPR alapján információt kell szolgáltatniuk a felügyeleti hatóságok felé tevékenységükkel kapcsolatban, ahogy az a felügyeleti hatóságok oldaláról már a IV.3.1. pontban említésre került. Abban az esetben, ha egy tanúsító szervezet tanúsítvány állít ki, újít meg, vagy visszavon, akkor ennek tényét és okait közölnie kell az illetékes felügyeleti hatósággal.[149] Ez a kötelezettség teszi lehetővé, hogy a felügyeleti hatóság rálásson a tanúsítási szervezet tevékenységére, és adott esetben gyakorolni tudja azt a hatáskörét, hogy utasítsa a tanúsító szervezetet a tanúsítvány visszavonására, vagy megtagadására.

---

145 EN-ISO/IEC 17065/2012 szabvány 3.12..

146 GDPR 42. cikk (5) bekezdés és 43. cikk (1) bekezdés.

147 GDPR 43. cikk (1) bekezdés.

148 Európai Adatvédelmi Testület: Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

149 GDPR 42. cikk (1) bekezdés és 43. cikk (5) bekezdés.

4.5. A tanúsító szervezetek akkreditálása

Tanúsítást a GDPR alapján a felügyeleti hatóság vagy tanúsító szervezet állíthat ki, ez utóbbi csak abban az esetben, ha akkreditált, vagyis ha megállapítják róla, hogy a lefolytatni kívánt tanúsítás vonatkozásában megfelel a jogszabályban és egyéb releváns dokumentumokban előírt követelményeknek. Az akkreditálás ugyanis „annak hivatalos elismerése, hogy egy szervezet, természetes személy alkalmas bizonyos megfelelőségértékelési tevékenységek elvégzésére."[150]

Az akkreditálás lényege tehát az, hogy hatósági megállapítást nyújt egy tanúsító szervezet szakértelméről. Az Európai Parlament és a Tanács 765/2008/EK rendelete alapján akkreditálás: a nemzeti akkreditáló testület tanúsítása arról, hogy egy megfelelőségértékelő szervezet megfelel a meghatározott megfelelőségértékelési tevékenységek ellátásához a harmonizált szabványokban megállapított követelményeknek és amennyiben alkalmazandó, bármely további követelménynek, beleértve a vonatkozó ágazati szabályozásokban meghatározottakat is.

A GDPR szerinti akkreditálás annak a felügyeleti hatóság vagy akkreditáló hatóság általi igazolását jelenti, hogy egy tanúsító szervezet alkalmas arra, hogy a GDPR szerinti tanúsítást állítson ki, figyelembe véve az EN-ISO/IEC 17065/2012 szabványt, illetve a felügyeleti hatóság vagy a Testület által megállapított kiegészítő követelményeket.

Az akkreditálás során az akkreditálást végző szerv azt vizsgálja meg, hogy egy adott tanúsító szervezet alkalmas-e egy konkrét tanúsítás lefolytatására. A GDPR esetén tehát ez azt jelenti, hogy megvizsgálja, a tanúsító szervezet alkalmas-e arra, hogy egy adatkezelő vagy adatfeldolgozó által végzett adatkezelési műveletet tanúsítson jóváhagyott szempontok alapján. A pozitív kimenetelű vizsgálat eredménye az akkreditált státuszra vonatkozó határozat, amelyben ezt az alkalmasságot megállapítja a hatáskörrel rendelkező szerv.

A GDPR úgy rendelkezik, hogy az akkreditációt legfeljebb ötéves időtartamra lehet megadni, és az azonos feltételek mellett megújítható, amennyiben a tanúsító szervezet teljesíti a követelményeket.[151]

A GDPR meghatározza, hogy ki végezheti a tanúsító szervezetek akkreditálását. Ezzel kapcsolatban több lehetőséget is megfogalmaz, melyek közül a tagállamok választhatnak, meghatározva azt, hogy az adott tagállamban mely szerv(ek) végezhetnek GDPR alapján akkreditálást. Ezt a választást nemzeti jogszabályban rögzítik.

A nemzeti jogalkotók az általános adatvédelmi rendelet alapján az alábbi három opció közül választhattak, vagyis a tagállamokban tanúsító szervezet akkreditációjára az alábbi módokon kerülhet sor:

1) az illetékes felügyeleti hatóság a saját maga által meghatározott követelmények alapján végzi az akkreditálást;
2) a 765/2008/EK európai parlamenti és tanácsi rendelet által megnevezett nemzeti akkreditáló testület végzi az akkreditálást, az EN-ISO/IEC 17065/2012 szabványban, és a felügyeleti hatóság által meghatározott kiegészítő követelményekben foglaltak alapján;
3) mind az illetékes felügyeleti hatóság, mind az akkreditáló testület végezhet akkreditálást, az előző két esetben meghatározott követelmények alapján.[152]

Amennyiben egy tagállamban a nemzeti akkreditáló testület végzi a tanúsító szervezetek akkreditálását (2-es és bizonyos esetben a 3)-as opció), a GDPR előírja, hogy ezt a fentebb említett ISO 17065-ös szabvány alapján kell végeznie, figyelembe véve a felügyeleti hatóságok által meghatározott kiegészítő

150 https://www.nah.gov.hu/mi-az-akkreditalas
151 GDPR 43. cikk (4) bekezdés.
152 GDPR 43. cikk (1) bekezdés.

követelményeket is. Emellett az akkreditáló testületeknek alkalmazniuk kell a 765/2008/EK rendeletet is tevékenységük során. A felügyeleti hatóságok által összeállított kiegészítő követelményeknek főleg a GDPR-ban megfogalmazott[153] követelményekre kell reflektálniuk, hiszen ezek specifikusan a GDPR szerinti tanúsító szervezetek akkreditálásával kapcsolatban határoznak meg követelményeket.

Ezek, a GDPR-ban a tanúsító szervezetekre vonatkozóan előírt követelmények a következők:

Egy szervezetet kizárólag abban az esetben lehet akkreditálni, ha:
- az illetékes felügyeleti hatóság számára kielégítő bizonyítékot szolgáltatott arra nézve, hogy független, és a tanúsítás tárgyában szakértelemmel bír;
- vállalja, hogy tiszteletben tartja az illetékes felügyeleti hatóság, illetve a Testület által jóváhagyott szempontokat;
- eljárásokat hozott létre az adatvédelmi tanúsítványok, bélyegzők, illetve jelölések kibocsátására, rendszeres időközönkénti felülvizsgálatára és visszavonására;
- olyan eljárásokat és struktúrákat hozott létre, amelyek révén kezelni tudja a tanúsítvánnyal kapcsolatos jogsértésekkel vagy annak az adatkezelő vagy adatfeldolgozó általi alkalmazásával kapcsolatos panaszokat, és ezeket az eljárásokat és struktúrákat az érintettek és a nyilvánosság számára átláthatóvá tudja tenni; és
- az illetékes felügyeleti hatóság számára kielégítő bizonyítékot szolgáltat arra nézve, hogy feladataival kapcsolatban nem áll fenn összeférhetetlenség.[154]

A felügyeleti hatóságok által kidolgozott, az EN-ISO/IEC 17065/2012 szabványt kiegészítő követelményeknek specifikus előírásokat kell tartalmazniuk, melyeknek fő célja, hogy megkönnyítsék az értékelését például annak, hogy egy tanúsító szervezet független, vagy megfelelő szakértelemmel bír az adatvédelem, és különösen az adott tanúsítás tárgya területén. Figyelemmel kell lenni ennek során ugyanis arra, ha egy tanúsítási mechanizmus például egy meghatározott szektor által alkalmazható, hiszen ilyen esetben a szakértelem meglétét is ehhez mérten kell megvizsgálni.[155]

A felügyeleti hatóságok által kidolgozott kiegészítő feltételek tervezetét közölni kell a Testülettel, amely arról véleményt bocsát ki. A Testület véleményét követően fogadhatja el a végleges követelményrendszert a felügyeleti hatóság. A kiegészítő követelményeket közzé kell tenni.[156]

Ha egy tagállamban az illetékes felügyeleti hatóság végezheti a tanúsító szervezetek akkreditálását [(1)-es opció], akkor maga állapíthatja meg ennek követelményeit. Ezzel kapcsolatban a fent felsorolt követelmények találhatók magában a GDPR-ban, de ezek nem teljes körűek, illetve ezekkel kapcsolatban nem utal a jogszabály az említett szabványra sem. Az egységesség érdekében ezért a felügyeleti hatóság által végzett akkreditálás esetén is irányadónak kell tekinteni az EN-ISO/IEC 17065/2012 szabványt, illetve a kiegészítő követelményeket.[157]

Magyarországon a 2018. évi XXXVIII. törvénnyel módosított, a nemzeti akkreditálásról szóló 2015. évi CXXIV. törvény (a továbbiakban: NAH tv.) alapján a GDPR szerinti tanúsító szervezet akkreditációját a Nemzeti Akkreditáló Hatóság végzi, azonban ebben részt vesz a NAIH is. Az akkreditálást azon adatvédelmi tanúsító szervezet kérheti, amely megfelel a GDPR-ban meghatározott szervezeti, személyi és működési követelményeknek. Az adatvédelmi tanúsító szervezet akkreditálására, illetve az akkreditált státusz bővítésére irányuló eljárásban az értékelési szakasz során a NAIH-ot szakhatóságként kell bevonni, a GDPR 43. cikk (2) bekezdésben, illetve

153 GDPR 43. cikk (2) bekezdés.

154 GDPR 43. cikk (2) bekezdés.

155 Európai Adatvédelmi Testület: Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679); 2019. június 4.

156 GDPR 57. cikk (1) bekezdés p) és 64. cikk (1) bekezdés c).

157 Európai Adatvédelmi Testület: Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679); 2019. június 4.

a kiegészítő követelményekben meghatározott szakkérdések tekintetében. A szakhatósági eljárás ügyintézési ideje 50 nap. Az akkreditálási eljárásért, illetve az akkreditált státusz területének bővítési eljárásért is igazgatási szolgáltatási díjat kell fizetni.[158] Az ilyen vegyes jellegű akkreditálási eljárás esetén, mint a magyar, ahol mind a nemzeti akkreditáló hatóságnak, mind a felügyeleti hatóságnak van szerepe, fontos, hogy a két szerv közötti feladatmegosztás és együttműködés részletei rögzítve legyenek.

Fontos még kiemelni, hogy az akkreditálást végző szervnek (nemzeti akkreditáló testület vagy felügyeleti hatóság) az akkreditálást követően is vannak feladatai: felügyeletet gyakorol a tanúsító szervezet felett, ellenőrzi annak tevékenységét, és amennyiben úgy ítéli meg, hogy nem vagy már nem felel meg a követelményeknek, vagy intézkedései megsértik a GDPR-t, akkor visszavonja az akkreditációt. Ez a hatáskör arra a szervre hárul, amelyet a tagállam az akkreditálás elvégzésére kijelöl.[159]

[158] NAH tv. 35–37. §.

[159] GDPR 43. cikk (7) bekezdés és NAH tv. 8–10. §.

5. IRODALOMJEGYZÉK

1. *Az Európai Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A személyes adatok cseréje és védelme a globalizált világban*, 2017.01.10. COM(2017) 7 final, URL: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017DC0007&from=EN Letöltés ideje: 2019. október 1.
2. Európai Adatvédelmi Testület: *2/2018. sz. iránymutatás az (EU) 2016/679 rendelet 49.cikke szerinti eltérésekről*, 2018. május 25., URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_hu.pdf Letöltés ideje: 2019. október 1.
3. Európai Adatvédelmi Testület: *1/2019 iránymutatás az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről*, 2019. június 4., URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_hu.pdf Letöltés ideje: 2019. október 1.
4. Péterfalvi Attila, Révész Balázs, Buzás Péter (szerk.): *Magyarázat a GDPR-ról*, Wolters Kluwer Hungary Kft., Budapest, 2018
5. Európai Adatvédelmi Testület: *9/2019. számú vélemény az Osztrák Adatvédelmi Hatóság által a magatartási kódexnek való megfelelést ellenőrző GDPR 41. cikk szerinti szervezet akkreditációjára vonatkozóan meghatározott szempontokról,* 2019. július 9., URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201909_ataccreditationrequirementsmonitoringbodies_en.pdf Letöltés ideje: 2019. október 1.
6. Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, Gabriela Bodea: *Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, Final Report, Európai Bizottság, 2019, URL: https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en Letöltés ideje: 2019. október 1.
7. European Union Agency For Network and Information Security: *Recommendations on European Data Protection Certification,* 2017. november, URL: https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification Letöltés ideje: 2019. október 1.
8. Európai Adatvédelmi Testület: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*, 2019. június 4., URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf Letöltés ideje: 2019. október 1.
9. Európai Adatvédelmi Testület: *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, 2019. június 4., URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf Letöltés ideje: 2019. október 1.
10. https://www.nah.gov.hu/mi-az-akkreditalas

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert rektorhelyettes

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Dorogi Katalin

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-268-5 (elektronikus)