



PÁZMÁNY *1635*
— *a l a p i t v a*

Pázmány Law Working Papers

2016/26

Szabó Endre Győző

**Az Európai Unió általános adatvédelmi
rendeletének egyes kérdéseiről I.**

**Az adathordozhatóság és az
adatvédelmi hatásvizsgálat**

Pázmány Péter Katolikus Egyetem
Pázmány Péter Catholic University Budapest

<http://www.plwp.eu>

Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről I.

Az adathordozhatóság és az adatvédelmi hatásvizsgálat

Az Európai Unió új adatvédelmi szabályai

Az Európai Bizottság 2012-ben nyújtotta be javaslatát egy új adatvédelmi keretre nézve. Az Európai Unió két társ jogalkotó szerve négy év tárgyalás után hagyta jóvá a két jogalkotási aktusból álló csomagot:

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

A most kezdődő íráskor sorában az első jogalkotási aktust, az általános adatvédelmi rendeletet ¹ vizsgáljuk. A sorozat első részében a jogalkotói célokkal és kiemelten az adatok hordozhatóságával, mint új érintetti jogosultsággal, valamint az előzetes adatvédelmi hatásvizsgálattal foglalkozunk.

¹ A rendeletet gyakran GDPR-ként (General Data Protection Regulation rövidítése) is említik, akár magyar nyelvű dokumentumokban, illetve közegben is.

A rendelet megalkotásáról

A rendelet elfogadásához az elsődleges jog, az Európai Unió Működéséről szóló Szerződés (EUMSZ) 16. cikke nyújtja a jogalkotási felhatalmazást. A cikk szerint a személyes adatok védelmére és az ilyen adatok szabad áramlására vonatkozó szabályokat rendes jogalkotási eljárás keretében az Európai Parlament és a Tanács állapítja meg. E szabályok tiszteletben tartását független hatóságok ellenőrzik.

A Bizottság e felhatalmazás alapján irányelvet és rendeletet is benyújthatott volna, de már a javaslat nyilvánossá válása előtt szakmai konszenzus mutatkozott abban, hogy a 95/46/EK számú adatvédelmi irányelv tapasztalatai alapján inkább az erősebb jogharmonizációt szolgáló rendeletre van szükség. Az EUMSZ 288. cikke szerint a rendelet általános hatállyal bír. Teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban. Ezt a szövegrészt a rendelet maga is megismétli, ezzel zárul a normaszöveg.

A rendelet az erősebb harmonizáció eszköze, a normaszöveg nem igényel tagállami átültetést, mindenki köteles az azzal összhangban lévő magatartás tanúsítására a tagállami jogalkotástól függetlenül.

A rendelet hatálya általános, az alól csupán meghatározott esetkörök mentesülnek, így például azok az adatkezelések, amelyek az Európai Unió joga alól egyébként is kivett témakörök. Itt említhetjük például a nemzetbiztonságot. A mentesülő területeken túl a rendelet általában és közvetlenül alkalmazandó jelleggel fogja szabályozni az életviszonyokat, ideértve az üzleti és közigazgatási adatkezeléseket is. Érthető, hogy az egyes érdekérvényesítésre szakosodott szervezetek kiemelt érdeklődéssel kísérték a jogalkotási folyamatot. Egybehangzó vélemények szerint az Uniónak ez volt a leginkább lobbival befolyásolt jogalkotási folyamata eddigi története során.

A korábbi jogi keret kritikája

Az új rendelet preambulum bekezdéseiben a korábbi adatvédelmi irányelv meglehetősen részletes és éles kritikáját olvashatjuk. Mintha az Európai Bizottság azon érvei lennének összefoglalva, amellyel a jogalkotó szervezetet a megválasztott jogalkotási aktus típus (rendelet) helyességéről kívánna meggyőzni.

A (9) preambulum bekezdés szerint az irányelv széttagolt módon valósult meg a tagállamokban, ez jogbizonytalanságot eredményezett, széles körben alakult ki az a benyomás, hogy az online környezetben a természetes személyeket kockázatok fenyegetik. Az eltérő védelmi szinteket eredményező tagállami átültetés az adatok szabad áramlásának útjában állhat, a gazdasági tevékenységek akadályát jelenthetik, amelyek torzítják a versenyt és az adatvédelmi felügyelő hatóságokat is hátráltatják feladataik végrehajtásában.

A rendelet kiindulópontjai

A rendelet lakóhelytől és állampolgárságtól függetlenül kíván ² védelmet biztosítani minden természetes személynek. A rendelet gazdasági természetű célkitűzései közé tartozik, hogy hozzá kíván járulni a gazdasági unió megteremtéséhez, a gazdasági és társadalmi fejlődéshez, a belső piacon belül a gazdaságok erősödéséhez, továbbá a gazdaságok konvergenciájához. Külön nevesített célja a

² A rendelet (2) preambulum bekezdése rögzíti ezt, a normaszöveg ezen túl explicit módon nem tér ki a személyi hatályra, csupán a tárgyi és a területi hatályt szabályozza.

rendeletnek, hogy hozzá kíván járulni a természetes személyek jólétéhez.³ Ennek háttérében és előfeltételeként olyan környezetre van szükség, ahol mind a jogalkotó, mind a joggyakorlatot alakító felügyeleti hatóság⁴ fogékony a piaci működéssel együtt járó folyamatokra. Ennek alapján ítéltethető meg, hogy melyek azok a tevékenységek, amelyek a jólétet szolgálják, és melyek azok, amelyek adott esetben már tisztességtelen és törvénytelen gyakorlatként értékelendők, ilyen módon pedig a jólét csökkenéséhez vezetnek. A gazdasági megfontolások értelemszerűen nem válnak a jogszerűség mércéjévé, mindenesetre a jogalkotó által kívánt módon a személyes adatok kezelését érintő ügyek mögött álló társadalmi-piaci folyamatok iránti fogékonyságot várnak el.

A jogalkotó a preambulumban hangsúlyozza, hogy a személyes adatok védelméhez való jog nem abszolút jog, hanem azt a többi jog fényében kell vizsgálni.⁵ A jogalkotó szándéka szerint a személyes adatok kezelését az emberiség szolgálatába kell állítani, ennek kapcsán pedig az adatvédelemnek a társadalomban betöltött szerepét hangsúlyozza. A személyes adatok kezelésének kontextusában nem csupán a kockázatokat, hanem azok révén az egyéni és közösségi jólét növelésének lehetőségét is értékelni kell. Ez az a mérce, amely normatív tartalommal nem bír ugyan, de át kell hatnia a rendelet alkalmazását.

A rendelet az előírt szabályok alkalmazását az adott keretek között várja el, számolva a technológia fejlődésével és a globalizációval együtt járó társadalmi, valamint gazdasági változásokkal. Az új technológiák nem jók vagy rosszak, hanem olyan körülmények, amelyeket figyelembe kell venni a jogalkotás és a jogalkalmazás során is.⁶

A jogalkotó azzal a szándékkal alkotta meg a rendeletet, hogy az következetesebb legyen, mint az irányelv szétaprózódott tagállami alkalmazása volt. Ennek jegyében olyan kikényszeríthetőséget kínál, amely hozzájárul a bizalom erősítéséhez. Ez a bizalom nélkülözhetetlen a digitális gazdaság belső piaci fejlődéséhez. Ennek érdekében egyenértékű hatáskört biztosít a tagállami hatóságoknak, és egységesíti a szankciókat is. Minden hatóság ugyanolyan eszköztárral rendelkezik, ez is egy fontos komponense annak, hogy az adatok forgalmának korlátozása érdekében nem lehet arra hivatkozni, hogy az egyik tagállamban magasabb vagy éppen alacsonyabb a védelem szintje.⁷

A rendelet hatályba lépése, illetve alkalmazandósága

A magyartól eltérő uniós jogi terminológia miatt tisztázást igényel, hogy mikortól kell alkalmazni a rendeletet. A (171) preambulumban bekezdés szerint a rendelet alkalmazásának időpontja előtt megkezdett adatkezelést a rendelet hatálybalépésének időpontjától számított két éven belül összhangba kell hozni a rendelettel. A rendelet az uniós terminológia szerint már hatályos, a rendelet maga rendelkezett így 99. cikkében: „ez a rendelet az Európai Unió Hivatalos Lapjában való kihirdetését követő huszadik napon lép hatályba”. A rendeletet 2016. május 4-én hirdették ki, május 24-én tehát hatályba lépett. Alkalmazandóvá azonban csak 2018. május 25-től válik, erről megint csak a rendelet szövege (a 99. cikk (2) bekezdése) rendelkezik.

³ A rendelet (2) preambulumban bekezdése.

⁴ A rendelet a felügyeleti hatóság elnevezést (supervisory authority) használja az irányelvben szereplő adatvédelmi hatóság (data protection authority) helyett.

⁵ A rendelet (4) preambulumban bekezdése.

⁶ A rendelet (6) preambulumban bekezdése.

⁷ Megjegyzendő, hogy ez az elvárás már a 95/46/EK irányelvben is szerepelt, teljes mértékben azonban kétségtelenül nem valósult meg.

Régi és új definíciók, elvek és jogalapok

Az alapfogalmak terén számos definíció változatlan tartalommal marad hatályban, ugyanakkor számos új fogalom is került a normaszövegbe. Az adatfeldolgozás fogalmát törölni kell a magyar adatvédelmi szótárból, a rendelet alkalmazása során csupán adatkezelésként jelölendő a személyes adatokon végzett bármely művelet. Az adatkezelő és az adatfeldolgozó fogalompár mindazonáltal megmarad. Új fogalomként definiálja a rendelet a profilalkotást, az álnevesítést, az adatvédelmi incidenst (a magyar jogalkotó már kodifikálta ezt, azonban az irányelvben nem volt ilyen definíció), a tevékenységi központot. Az adatok zárolása helyett az adatkezelés korlátozásához való jogot említi a rendelet.

Az átláthatóság hangsúlyozása az egyik újdonsága a rendeletnek. Az elmúlt években gyakran esik szó az adatvédelem, a versenyjog és a fogyasztóvédelem kapcsolatáról. E három terület metszetében az egyik elvárás az átláthatóság követelményének az érvényesítése.

Az elszámoltathatóság elve új elvként két elvárást rögzít: egyrészt azt várja el az adatkezelőtől, hogy a saját szervezetén belül alakítsa ki a megfelelő folyamatokat annak érdekében, hogy a rendeletnek való megfelelést szavatolni tudja, másrészt az arra való képességet várja el kötelező jelleggel, hogy ezt kérésre be is tudja mutatni.

A jogalapok terén az irányelvhez képest nincsen jelentős változás, továbbra is az érintett hozzájárulása, szerződés teljesítése, jogi kötelezettség teljesítése, az érintett létfontosságú érdekének védelme, közhatalmi jogosítvány gyakorlása és az adatkezelő jogos érdekének érvényesítése szolgálhat az adatkezelés alapjául.

A továbbiakban a rendelet újításai közül emeljük ki azokat, amelyek a magyar jogalkalmazás szempontjából is kiemelt figyelmet érdemelnek.

Az adathordozhatóság (data portability)

Az adatok hordozhatóságát új jogosultságként vezeti be a rendelet.⁸ Sem az irányelv, sem a magyar jog nem ismerte ezt az érintetti jogosultságot eddig. A jogosultság célja, hogy a személyes adatok feletti rendelkezést tovább erősítse.

A technológia nyújtotta lehetőségeket, a kommunikációs szokások átalakulását a jogalkotó figyelembe veszi. Ilyen sajátosságok a dolgok internete, az okos mérők, a cloud computing, az elektronikus kommunikáció tömegessé válása vagy éppen a mobil applikációk használata.

Az új jogosultság tartalma

Az adathordozhatóság alapján az érintettnek joga van arra, hogy az adatokat megkapja, használja, illetve egy másik adatkezelőnek továbbítsa, vagy azt kérje, hogy egy másik adatkezelőnek továbbítsák. E jogát akkor gyakorolhatja, ha az érintettre vonatkozó adatokról van szó, és az érintett bocsátotta az adatkezelő rendelkezésére.

⁸ A rendelet 20. cikke szabályozza, indokolást, valamint értelmezést a (68) preambulum bekezdés fűz hozzá

A jog gyakorlása számos feltételhez kötött: akkor gyakorolható, ha az adatkezelés jogalapja az érintett hozzájárulása, vagy szerződés keretében bocsátották azokat rendelkezésre. Más jogalapon alapuló adatkezelés esetében az adathordozhatóság joga nem gyakorolható. Ezen túl csupán automatizált adatkezelés esetében hivatkozhat az érintett e jogosultságára.

A normaszöveg tartalmaz olyan kifejezéseket, amelyek értelmezésre szorulnak. Ilyen a géppel olvashatóság és az interoperabilitás (átjárhatóság).

A géppel olvashatóság definícióját megtaláljuk a 2013/37/EU számú irányelvben a közsféra információinak további felhasználásáról⁹: „Egy dokumentum akkor tekinthető számítógéppel olvasható formátumú dokumentumnak, ha olyan fájlformátumú, amely lehetővé teszi a szoftveres alkalmazások számára, hogy a benne lévő egyedi adatokat könnyen azonosítsák, felismerjék és kinyerjék. A számítógéppel olvasható formátumban létrehozott fájlokban kódolt adatok számítógéppel olvasható adatoknak tekintendők.”

Az interoperabilitásra is van definíciója az Európai Unió jogának, az európai közigazgatások közötti átjárhatósági eszközökről szóló 2009/922/EK határozatában. E szerint átjárhatóság: az eltérő és különböző szervezetek együttműködési képessége a kölcsönösen hasznos és kölcsönösen megállapított közös célok érdekében, ideértve az információk és ismeretek megosztását a szervezetek között az általuk támogatott munkafolyamatokon keresztül, a saját információs és kommunikációs rendszereik közötti adatcsere segítségével.

Tekintettel arra, hogy ezek a fogalmak tisztázottak, nem szükséges további iránymutatás az adatvédelmi felügyeleti hatóságok részéről azok tartalmát illetően.

A jog gyakorlásának feltételeit illetően adódik a kérdés, hogy az adatkezelőknek köteleességük-e az adathordozhatóságot lehetővé tevő átjárható formátumok fejlesztése? Ez nem kötelezettség, de az adatkezelőket erre „ösztönözni kell” a rendelet alapján.

Értelmezési tartományok

Az adathordozhatóság alkalmazásának terjedelmére nézve a normaszöveg alapján eltérő értelmezési tartományok mutatkoznak. A „rá vonatkozó” kitétel, továbbá az „általa rendelkezésre bocsátott” fordulat szűkebb és tágabb értelmezésnek is teret enged. Az adatvédelmi hatóságok várhatóan a lehető legszélesebb értelmezést szeretnék majd érvényesíteni, míg a legszűkebb értelmezés szerint kívül esne a jog által szabályozott esetkörön például az e-mail, mert nem kizárólag az érintettre vonatkozó adat van benne, vagy a közösségi oldal profilja is ugyanilyen megítélés alá esne, hasonló okokból.¹⁰

További korlátokkal is számolnia kell a joggyakorlás során az érintettnek, ugyanis nem gyakorolható a közhatalmi feladataikat gyakorlókkal szemben. Így értelemszerűen például az ügyfélkapu alkalmazása kapcsán rögzített adatok nem eshetnek e szabály alá.

⁹ Az irányelv (21) preambulum bekezdésében

¹⁰ A jelenleg folyó egyeztetések során elemzik az e-mail postafiók, a digitálisan rögzített elérhetőségi adatok listáját, a csoportos chat üzenetek sorsát, a blogokat és az azok kapcsán született posztokat, továbbá a banki tranzakciók adatai és az internetes ügyintézés során megadott információk (például egy biztosítási kötvényhez szükséges adatok) esetében az adathordozhatóság gyakorolhatóságát.

A rendelet abból indul ki, hogy e jogát az érintett gyakorolja. Számol azzal a konfliktussal, hogy ez adott esetben mások jogait is érintheti. Erre az esetre a preambulum bekezdés azt az iránymutatást adja, hogy „ha egy adott személyes adatállomány egynél több érintettre vonatkozik, a személyes adatok megszerzéséhez való jog nem sértheti az egyéb érintettek e rendelet szerinti jogait”. Nem adódhat tehát olyan helyzet, amelynek eredményeként az adathordozás révén más érintett hátrányosabb helyzetbe kerül. Mivel itt az érintett rendelkezéséről van szó, akivel szemben a transzparencia követelménye nem fogalmazódik meg (hiszen a saját adatait illetően nem adatkezelő), feltehetően az adatok útjának követhetővé tétele érdekében tartotta szükségesnek a jogalkotó ennek a korlátnak a beépítését.

Az adathordozhatósághoz való jogtól függetlenül gyakorolható az adatok törléséhez való jog, ennek gyakorlása értelemszerűen nem járhat más adatalany jogainak kiüresítésével (hogy ne gyakorolhassa az adatok törléséhez való jogát, vagy az adatok kezelésének korlátozására való igényét ne érvényesíthesse). Erre a kérelem érvényesítése során figyelmet kell fordítani, és az adatkezelőnek kell garantálnia, hogy ez a kívánalom érvényesüljön.

A jog technikai kivitelezésének részleteit illetően minden adatkezelőnek magának kell felkészülnie, de várható, hogy széles körben kerül a jog alkalmazása megvitatásra, amely a rendelet alkalmazásáig hátra lévő közel két évben kellő iránymutatásul fog szolgálni az adatkezelők számára.

Adatvédelmi hatásvizsgálat¹¹ (privacy impact assessment)

Az adatvédelmi hatásvizsgálat lényege az adatkezelés előzetes kontrollja a kockázatok feltárása és a kockázatok mérséklésére teendő intézkedések értékelése révén.

A kockázat azonosítása

Kulcskérdés, hogy a rendelet alkalmazásában mit tekintünk kockázatnak. A rendelet preambulum bekezdései adnak iránymutatást ebben a tekintetben. A (75) bekezdés szerint a természetes személyek jogait érintő kockázatok származhatnak a személyes adatok kezeléséből, amelyek eredménye lehet fizikai, vagyoni, nem vagyoni kár, hátrányos megkülönböztetés, személyazonosság lopás, vagy személyazonossággal való visszaélés, szakmai titoktartási kötelezettség által védett személyes adat bizalmas jellegének sérülése, az álnevesítés engedély nélküli feloldása, gazdasági vagy szociális hátrány. További következmény lehet, hogy az érintettek nem gyakorolhatják jogaikat, vagy nem rendelkezhetnek saját személyes adataik felett, vagy olyan személyes adatok kezelése történik, amely faji vagy etnikai származásra vagy politikai véleményre, vallási, illetve világnézeti meggyőződésre, szakszervezeti tagságra utal. A kockázatok közé sorolandó, ha az adatkezelés genetikai adatokra, egészségügyi adatokra, a szexuális életre, a büntetőjogi felelősség megállapítására vonatkozik, továbbá ha a személyes jellemzők értékelésére, így a munkahelyi teljesítmény, gazdasági helyzet, egészségi állapot, személyes preferenciák, érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére és előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából. Külön nevesített kategóriája a kockázatnak, ha kiszolgáltató személyek, különösen, ha

¹¹ Az új jogintézményt a rendelet 35. és 36. cikke szabályozza, a (75), (76), (77), (83), (84) preambulum bekezdések kapcsolódnak hozzá.

gyermekes személyes adatainak kezelésére kerül sor, továbbá ha az adatkezelés nagy mennyiségű személyes adat alapján történik és nagyszámú érintettre terjed ki.

A hatásvizsgálat előkészítésének következő kérdése, hogy miként elemezze az adatkezelő, hogy a konkrét esetben, ha a kockázat esélye fennáll – márpedig a felsorolás során az adatkezelések jelentős része esetében definiálható lesz kockázat – annak súlyosságát, illetve valószínűségét. A rendelet maga ad néhány fogódzót erre az esetre: az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell megállapítani, hogy a kockázat valószínűsíthetően magas, erre utalhat továbbá az új technológia alkalmazása különösen. Ezt követően a rendelet preambuluma olyan objektív értékelésre utal, amelynek részletei a rendeletben már nem találhatók meg. Itt nyilvánvaló szerepe lesz az olyan iránymutatásoknak, amelyek az adatvédelmi hatóságoktól, illetve az Európai Adatvédelmi Testülettől (Testület) várhatók.¹²

A kockázatok mérséklésére irányuló intézkedések

A kockázatok azonosítását követően a kockázatok mérséklésére irányuló intézkedések számbavétele az adatkezelő feladata. Itt a rendelet ismét csak utal bizonyos támpontokra, így bevált gyakorlatokra, amelyek például jóváhagyott magatartási kódexekben lelhetők fel, továbbá a tanúsítási eljárásokra, a Testület iránymutatásaira, valamint az adatvédelmi tisztviselő által házon belül nyújtott iránymutatásokra. A rendelet a kockázatok mérséklésére irányuló intézkedések között több helyen is említi az adatok álnevesítését, mint lehetséges intézkedést.

A jogbiztonság terén nem csupán az azonosított magas kockázatokra, és ezek mérséklésére vonatkozó iránymutatások fognak fontos szerepet játszani, hanem azok a dokumentumok is, amelyek a valószínűsíthetően magas kockázattal nem járó adatkezelési műveleteket mutatják be. A Testület például meghatározhatja, hogy melyek ezek, és azt is, hogy mely intézkedések elegendők a kockázatok mérséklésére.

Az adatvédelmi hatásvizsgálat alá eső adatkezelések

Az általános szabály szerint azon adatkezelések tekintetében kell elvégezni az adatvédelmi hatásvizsgálatot, amelyek a fentiek alapján valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve, és ezek az adatkezelő által elvégezni kívánt intézkedések ellenére sem küszöbölhetők ki. A vizsgálat elvégzése az adatkezelő kötelezettsége, amelynek elvégzésekor az adatvédelmi tisztviselő tanácsát ki kell kérni, ha van kijelölt tisztviselő.

Azt, hogy mely esetekben kell majd előzetes adatvédelmi hatásvizsgálatot végezni, alapvetően a felügyelő hatóságok, valamint a Testület fogja majd meghatározni. A rendelet három esetkört emel ki, amikor a vizsgálat elvégzése kötelező: (1) automatizált adatkezelések, amelyek személyes jellemzők kiértékelésén alapuló olyan döntésekhez vezetnek, amelyek a természetes személyeket jelentősen érintik, többek között rájuk nézve joghatással bírnak; (2) a rendelet alapján meghatározott különleges adatkategóriába tartozó személyes adatok, valamint a büntetőjogi felelősséggel összefüggő információk kezelése; (3) nyilvános helyek nagymértékű, módszeres megfigyelése.

¹² Az új adatvédelmi rendelet szerint az EGT adatvédelmi hatóságait az Európai Bizottság tanácsadó szerveként működő, az irányelv 29. cikke alapján létrehozott Munkacsoportot felváltja a Bizottságtól független, nem csupán tanácsadó, hanem döntéshozatali jogosultságokkal is felruházott Európai Adatvédelmi Testület.

Az első esetkör elsősorban az ún. scoring rendszerű értékelésekre vonatkozik, amelyek például a hitelbírálatok vagy a munkahelyi teljesítmény értékelése alapján jelentős mértékben befolyásolhatják a természetes személyek helyzetét, érvényesülését. A második és a harmadik kategória nem igényel külön magyarázatot, hiszen a jogi fogalmak tisztázottak. Mindazonáltal meg kell jegyezni, hogy a jelenlegi magyar szabályozás is beépített ezek kapcsán bizonyos garanciákat. Az egészségügyi intézményrendszerben a húsz főnél nagyobb egységeknél kötelező belső adatvédelmi felelős kinevezése,¹³ a közterületi térfigyelő rendszerek esetében pedig a rendőrségről, valamint a közterület-felügyeletről szóló törvény ír elő egy sajátos engedélyezési eljárást, amelybe az érintett területen lakók képviselői döntenek (az önkormányzati képviselő-testület).¹⁴

Listák a hatásvizsgálat alá eső, valamint az alól mentesülő adatkezelésekről

A felügyelő hatóságnak össze kell állítania egy olyan listát, amely a hatásvizsgálat alá tartozó adatkezeléseket sorolja fel. Annak a listának az összeállítása, amely a hatásvizsgálat alól mentesülő adatkezeléseket sorolja fel, nem kötelezettség, pusztán lehetőség a hatóság számára. A hatásvizsgálat hatékony alkalmazásának előfeltétele, hogy a hatóságok összehangolják tevékenységüket ezen a téren, ezért a rendelet előírja, hogy a jegyzékek elfogadását megelőzően az egységességi mechanizmus keretében egyeztessenek egymással, ha több tagállamra kiterjedő hatása lehet az adatkezelésnek, illetve emiatt érintheti a személyes adatok Unión belüli szabad áramlását. Ettől függetlenül egyéb esetekben is kívánatos, hogy a hatóságok egyeztessenek egymással, hiszen kerülendő az a helyzet, amikor egy adatkezelés típus egy tagállamban hatásvizsgálat alá esik, míg egy másikban mentességet élvez. Tekintettel a terület komplexitására, a szükséges egyeztetések hosszára, 2018 tavasza előtt várhatóan nem fognak megjelenni ezek a listák a nyilvánosság előtt.

Megjegyzendő, hogy az előzetes adatvédelmi hatásvizsgálat elvégzésének követelménye adott esetben jelentős terhet jelent az adatkezelő szervezet számára. Ennek alapján a hatóságoknak csupán azokat az adatkezeléseket célszerű ilyen kötelezettség alá vonni, amelyek valóban olyan kockázatokat hordoznak, amelyek mérséklése nagy körültekintést és felkészültséget igényel. A rendelet a kis- és közepes méretű vállalkozások esetében az adminisztratív terheket a lehető legalacsonyabb szinten szeretné tartani, ezért azzal is számolni lehet, hogy e szektor bizonyos esetekben mentességeket, könnyítéseket fog kapni a többi adatkezelőhöz képest.

Elszámoltathatósági eleme a szabályozásnak, hogy a hatásvizsgálat során figyelembe kell venni, ha az adatkezelő teljesíti a rendelet értelmében jóváhagyott magatartási kódex előírásait. Az érintettek bevonását véleményük kikérése révén támogatja a rendelet akkor, amikor kereskedelmi érdekek, a közérdek vagy a biztonság sérelme nélkül van erre lehetőség. Az adatalanyok, valamint az ő képviselőik bevonása a hatásvizsgálat elkészítésébe tehát nem kötelezettség.

A rendelet az ún. mikro szinten végrehajtott adatkezelési műveletek előzetes adatvédelmi hatásvizsgálatáról rendelkezik. Abban az esetben, ha az adatkezelés jogalapja a rendelet 6. cikk (1) bekezdésének c) és e) pontja szerint (az adatkezelés jogi kötelezettség teljesítése céljából, valamint közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásához szükséges) uniós vagy tagállami jog írja elő, akkor nem szükséges az adatvédelmi hatásvizsgálatot elvégezni. Ennek feltétele,

¹³ Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 32. § (4) bekezdése szerint

¹⁴ A Rendőrségről szóló 1994. évi XXXIV. törvény 42. §-ában szabályozott eljárás.

hogy a jogalap elfogadása során, tehát a jogalkotási folyamatba építve egy általános hatásvizsgálat keretében már adatvédelmi vizsgálatot is végeztek. A tagállamok még ebben az esetben is rendelkezhetnek úgy, hogy az adatvédelmi hatásvizsgálatot az egyes adatkezelések megkezdése előtt el kell végezni.

Az adatvédelmi hatásvizsgálat felülvizsgálata

A rendelet csak két iránymutatást nyújt az elvégzett adatvédelmi hatásvizsgálatok felülvizsgálata kapcsán: egyrészt szükség szerint kell elvégezni, másrészt legalább akkor, amikor a kockázat változik. Ez számos körülmény miatt bekövetkezhet, például megnő az érintettek száma, vagy bármilyen olyan új körülmény adódik, ami a kockázatokról szóló felsorolásban szereplő körülmények jelentős változásával járnak.

Konzultáció az adatvédelmi hatósággal

Ha az előzetes adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés valószínűsíthetően magas kockázattal jár, az adatkezelés megkezdése előtt konzultálni kell a hatósággal. Ez a konzultációs kötelezettség akkor is fennáll, ha az adatkezelő egyébként nem csupán a kockázatokat, hanem az azok mérséklésére teendő intézkedéseket is azonosította.

A hatóság az adatkezelő konzultációs kérelmére a rendeletben meghatározott határidőben válaszol, és ha úgy látja, hogy nem elégséges módon azonosították a kockázatokat, vagy azokat nem megfelelő módon csökkentenék, írásban ad tanácsokat az adatkezelőnek. Ettől függetlenül gyakorolhatja egyéb hatásköreit is, így például a hatóság megtilthatja az adatkezelést. A konzultáció során az adatkezelő minden olyan információt a hatóság rendelkezésére bocsát, amely az adatkezelés jogszerűségének megítéléséhez szükséges.

Jogszabályok véleményezése és az adatkezelések engedélyezése

Az előzetes adatvédelmi hatásvizsgálat kapcsán a rendelet még két esetkört szabályoz: előírja, hogy a jogalkotó a személyes adatok kezeléséhez kapcsolódó jogalkotási javaslatok kapcsán szerezzék be a hatóság előzetes véleményét, továbbá a közérdek alapján ellátandó feladatok kapcsán megengedi, hogy a tagállami jog az ilyen adatkezelések előtt a hatóság engedélyének beszerzését írja elő.

Mindezek az intézkedések a beépített adatvédelem (privacy by design) elvének gyakorlati megvalósulását szolgálják.

Utólagos hatásvizsgálatok lehetősége a rendelet alapján

Kérdésként adódik, hogy lesz-e lehetőség vagy kötelezettség a rendelet alkalmazását megelőzően megkezdett adatkezelések utólagos vizsgálatára? A rendeletnek nincs visszaható hatálya, ezért a felügyelő hatóságok bizonyosan nem fogják az adatkezelőket arra kötelezni, hogy utólag végezzenek a jogszabály által előzetesen elvárt vizsgálatot. Mit tehet az adatkezelő, ha mégis garanciát keres az adatkezelés jogszerűségét illetően 2018. május 25-ét követően? Egyelőre az prognosztizálható, hogy a tagállami mozgástér lehetővé teszi a magyar adatvédelmi audithoz hasonló szolgáltatások megteremtését, illetve továbbélését. Ennek megfelelően a magyar adatvédelmi hatóság minden bizonnyal 2018 májusa után is fogad majd audit iránti kérelmeket, és a kérelmezett auditokat el fogja végezni.

Kérdés az is, hogy a rendelethez képest lesz-e részletes módszertan a hatásvizsgálat lefolytatására nézve? Olyan módszertan lenne a leghasznosabb, amely az Unió valamennyi tagállamában egységesen alkalmazható. Tekintettel a markánsan eltérő tagállami megközelítésekre, egyelőre nem látszanak egy lehetséges közös módszertan körvonalai.