Adatvédelmi tisztviselők 2019. évi konferenciája

Az adatvédelmi tisztviselőktől érkezett, a videós előadások keretében nem megválaszolt kérdések

1. „Internetes weboldalak cookie-k és hírlevelek kötelezően önkéntes bejelölése”

Az olyan sütik esetében, amelyek nem szükségesek egy honlap alapvető működéséhez vagy informatikai biztonságához, tehát például csak statisztikai, kényelmi, marketing célokat szolgálnak, a megfelelő jogalap a GDPR 6. cikk (1) bekezdés a) pontja szerinti hozzájárulás lehet.

A hozzájárulás érvényességéhez szükséges, hogy az a GDPR 4. cikk 11. pontja szerinti valamennyi kritériumnak megfeleljen, azaz az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása kell legyen, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

A GDPR általános szabályként rögzíti, hogy a hozzájárulás csak akkor tekinthető önkéntesnek, ha az érintettnek valódi választási lehetősége van, vagyis szabadon, kényszer nélkül dönthet a hozzájárulásának megadásáról, és nem kell semmiféle hátránytól vagy retorziótól tartania, amennyiben nem járul hozzá az adatkezeléshez vagy a hozzájárulását visszavonja.

Amennyiben az adatkezelő a szolgáltatáshoz való hozzáférés feltételeként szabja a hozzájárulás megadását, úgy kétséges, hogy számára a hozzájárulás a megfelelő jogalap, mivel ha az így kezelni kívánt személyes adat a szolgáltatás teljesítéséhez szükséges, úgy az adatkezelés megfelelő jogalapjául a GDPR 6. cikk (1) bekezdés b) pontja szolgálhat. Ellenkező esetben azonban, amikor az adatkezelő által kezelni kívánt személyes adatok nem szükségesek a szolgáltatás teljesítéséhez, de azt az adatkezelő mégis az adatkezeléshez való hozzájáruláshoz köti, úgy ez a kicsikart hozzájárulás nem tekinthető önkéntesnek, mivel az érintettet megfosztja a valódi választás lehetőségétől. Az adatkezelők hasonló helyzetekben gyakran hivatkoznak arra, hogy az általuk nyújtott szolgáltatás igénybevétele nem kötelező, ezért, ha az érintett saját döntése alapján mégis igénybe szeretné azt venni, úgy el kell fogadnia az adatkezelő által szabott feltételeket. Ez az érvelés azonban nem helytálló, mivel minden adatkezelőre – tevékenységétől függetlenül – egyformán vonatkoznak az adatvédelmi szabályok, így a személyes adatok kezelése csak megfelelő jogalap alapján történhet az alapelvek figyelembevétele mellett, ellenkező esetben az adatkezelő által végzett adatkezelés jogellenesnek minősül.

A hozzájárulás további érvényességi kritériuma, hogy az konkrét legyen. Ha az adatkezelés több különböző célból történik, úgy a hozzájárulást valamennyi adatkezelési célra vonatkozóan külön-külön kell megadni, amelyből az következik, hogy az érintettnek valamennyi adatkezelési cél vonatkozásában választási lehetőséget kell biztosítani. A GDPR célja a hozzájárulás konkrétságának megkövetelésével, hogy az érintett számára rendelkezési jogot biztosítson a személyes adatai felett, illetve átláthatóvá tegye számára az adatkezelést.

Ha az adatkezelő a honlapon nem ad lehetőséget az érintetteknek arra, hogy csak a választásuk szerinti célból alkalmazott sütik telepítését fogadják el és a sütik telepítését csak egységesen, valamennyi célra együttesen lehet elfogadni, azaz az adatkezelő nem biztosít választási lehetőséget

az érintetteknek, hogy mely sütik telepítését engedélyezik az eszközükön és melyeket nem, azzal sérül a hozzájárulás konkrétsága.

A hozzájárulást olyan módon kell beszerezni az érintettektől, hogy az az érintett akaratának egyértelmű kinyilvánítása legyen nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet formájában, amelyben beleegyezését adja az őt érintő személyes adatok kezeléséhez. Ezt nevezzük a hozzájárulás kifejezettségének.

Ha az adatkezelő felugró ablakban csak tájékoztatja az érintetteket arról, hogy a weboldalon cookie-kat használ, de nem ad lehetőséget arra, hogy az érintett választása szerint módosíthassa a beállításokat, úgy ez a megoldás nem felel meg a hozzájárulás érvényességéhez szükséges kifejezettség követelményének.

Jó megoldás lehet – a hozzájárulás kifejezettségének szempontjából –, hogy a felugró ablakban megjelenő szövegben az adatkezelő a különböző célokból alkalmazott sütik tekintetében külön-külön kéri a Kötelezett hozzájárulását, amelyet jelölőnégyzetek bejelölésével tudnak megadni az érintettek, egy megerősítő gombra kattintást követően.

2. „Követeléskezelés és befektetési tanácsadás esetén a rögzített hívások esetében a beszélgetés előtt a tájékoztatás adása minden esetben kötelező, olyan ügyfelek esetében is, akikkel naponta többször is, vagy nagyon rendszeresen van hívás?”

A hívás rögzítéséről a beszélgetés megkezdése előtti tájékoztatás az adatkezelők GDPR 13. cikke szerinti kötelezettsége. A GDPR 13. cikk (1) bekezdése szerint az adatkezelés lényeges körülményeiről a személyes adatok megszerzésének időpontjában kell tájékoztatást nyújtania az adatkezelőnek.

A GDPR 13. cikk (4) bekezdése úgy rendelkezik, hogy a 13. cikk (1)-(3) bekezdéseiben foglaltak nem alkalmazandók, ha és amilyen mértékben az érintett már rendelkezik az információkkal. Ezen jogszabályhelyre való hivatkozás esetén annak a bizonyítása, hogy az érintett milyen információkkal rendelkezik az adatkezelésről, az adatkezelő milyen információkat adott át a részére korábban, az adatkezelő feladata bizonyítani az elszámoltathatóság GDPR 5. cikk (2) bekezdése szerinti elve alapján.

A Hatóság álláspontja szerint a fent említett esetben – ügyféllel telefonon való rendszeres kapcsolattartás esetén, tehát minden egyes telefonhívás alkalmával – tájékoztatni kell az érintettet.

3. „Elektronikus úton (e-mail) történő érintetti joggyakorlás esetén mi a megfelelő személyazonosítási módszer? „

A GDPR 12. cikk (6) bekezdése szerint, ha az adatkezelőnek megalapozott kétségei vannak az érintetti joggyakorlásra irányuló kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

A további információk megadására való felszólítás nem lehet automatikus, az adatkezelőnek vizsgálnia kell, hogy a kérelemben foglaltak és a rendelkezésére álló további információk ismeretében ténylegesen van-e kétsége az érintett kilétével kapcsolatban.

Nem megalapozott a kétség például, ha a kérelem az adatkezelő által már az érintett e-mail címeként kezelt e-mail címről érkezik, én nem merül fel olyan ok, amely alapján az adatkezelőben megalapozott kétely merül fel a küldő személy kilétével kapcsolatban.

Ha megalapozott a kétség a kérelmet benyújtó kilétét illetően, akkor is csak olyan személyes adat megadása kérhető az érintettől, amelyet az adatkezelő már kezel, azaz a megadott adatot össze tudja hasonlítani egy nála már rendelkezésre álló adattal. Figyelembe kell venni az adattakarékosság elvét is a lehető legkevesebb erre alkalmas adat alkalmazásával, ami az adott adatkezeléstől függ. Lehetséges például a négy természetes személyazonosító adatok valamelyikéből, a lakcímből, és az ügyszámból kiválasztott adatok kombinációját használni.

(kapcsolódó ügy: NAIH/2019/1841)

4. „Amennyiben az ügyfél szerződésmásolatot, számlakivonatot vagy egyéb dokumentációt igényel, úgy azt mindenképpen a hozzáférési jog gyakorlásának kell-e tekinteni? Ha igen, úgy a másolatok kiadását úgy kell-e biztosítani, hogy az ügyfél adatain kívül a szerződést aláíró felek, kezesek és egyéb kötelezettek adatait ki kell húzni azért, hogy az ne érintse hátrányosan mások jogait és szabadságait?”

Az érintettet megilleti a másolathoz való jog, azonban az nem érintheti hátrányosan mások jogait és szabadságait.

A GDPR 4. cikk 1. pontja szerint személyes adat az azonosított vagy azonosítható természetes személyre vonatkozó bármely információ. A szerződések, számlakivonatok az ügyfél személyes adatának minősülnek, mivel azok az ügyfelet megillető jogosultságokra, őt terhelő kötelezettségekre, pénzügyi helyzetére vonatkoznak. A harmadik személyek személyes adatai – aláírás, kezesek adatai – az osztott személyes adatokat ide nem értve, azonban nem minősülnek az ügyfél személyes adatának.

Ennek kapcsán a Hatóság megjegyzi, hogy a hitelintézetek és a pénzügyi vállalkozások által az ügyfelekkel kötött szerződések kapcsán a Hpt. 279. § (1) bekezdése alapján az írásban kötött szerződés egy hiteles példányát a pénzügyi intézmény köteles az ügyfél rendelkezésére bocsátani. Amennyiben az ügyfél ezt az eredeti példányt elhagyja, vagy csak ellenőrizni akarja, hogy milyen adatait milyen dokumentumokban kezeli az adatkezelő, úgy nem feltétlenül szükséges a harmadik személyek személyes adatait a másolaton kitakarni, mivel ezen információk, személyes adatok korábban már az ügyfél tudomására jutottak, így az azokhoz való ismételt hozzáférés nem érinti hátrányosan a harmadik személyek jogait és szabadságait.

Kérdésként szokott felmerülni továbbá, hogy megtagadható-e másolat adása olyan dokumentumról, amely bár tartalmazza az érintett személyes adatait, de egyben az adatkezelő üzleti titkát is képezi. Itt fontos megjegyezni, hogy a hozzáférési jog a személyes adatra vonatkozik, amely önmagában nem képezheti üzleti titok tárgyát, így az üzleti titoknak minősülő információ kitakarásával ezen dokumentumokról is kell másolatot adni az érintettnek (adatelv – iratelv).

5. „Nagyobb adatbázissal és ügyfélnyilvántartással rendelkező cégek esetében napi/heti mentések készülnek az adatbázisról. A mentések x ideig külön adattároló lemezen kerülnek megőrzésre. Abban az esetben, ha egy érintett személyes adatait törölni kell, a külön tárolt mentett adatbázis tárolókról is egyesével törölni kell az adatait, vagy elegendő arra

hivatkozni, hogy azokat senki sem alkalmazza, senki sem fér hozzájuk és az általános elévülési szabályok szerint azok is törlésre kerülnek."

Amennyiben a GDPR 17. cikke szerint egy személyes adatot törölni kell, az azt jelenti, hogy a személyes adatot az adatkezelő nem kezelheti tovább. A GDPR 4. cikk 2. pontja szerint a személyes adatok tárolása is adatkezelésnek minősül, függetlenül attól, hogy az adatokhoz hozzáfér-e valaki vagy sem.

Az adatkezelőknek a GDPR 25. cikke szerinti beépített és alapértelmezett adatvédelem elve alapján megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére és tárolásuk időtartamára is.

A fentiek alapján az adatkezelőknek úgy kell kialakítaniuk a rendszereiket, hogy szükség esetén a biztonsági mentésekből is törölni tudja az érintettek személyes adatait.

6. „Online marketing, E-DM, címlistákkal kapcsolatos adatkezelés, hozzájárulás kérés megfelelő mechanikája, metódusa."

a) A hírlevélküldés leggyakoribb jogalapja a GDPR 6. cikk (1) bekezdés a) pontja szerinti[1] érintetti hozzájárulás.

A hírlevélküldési célú adatkezeléshez adott hozzájárulással kapcsolatban általánosságban érdemes megjegyezni, hogy a hozzájárulás úgy is megadható, hogy az érintett valamely internetes honlap megtekintése során aktív magatartással kinyilvánítja szándékát arra nézve, hogy hírlevelet kíván fogadni , így például bejelöl egy erre vonatkozó négyzetet vagy az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre. A hozzájárulás GDPR 4. cikk 11. pontja szerinti további követelményeinek természetesen ebben az esetben is érvényesülnie kell. A hozzájárulás érvényességének további követelményeit a Hatóság egy korábbi kérdésre adott válaszban már kifejtette.

Ebből kifolyólag az előre kipipált checkbox nem felel meg a hozzájárulás megadásával szemben támasztott követelményeknek, tekintettel arra, hogy előfordulhat olyan eset, amikor az érintett az adatai megadásakor nem veszi észre a már kipipált checkboxot, és így egy olyan nyilatkozatot tesz, amelyet nem biztos, hogy meg akart tenni.

Amennyiben a hírlevélküldés jogalapja – függetlenül attól, hogy a mi a hírlevélküldés célja – az érintett hozzájárulása, a GDPR alapján az érintett jogosult arra, hogy ezen hozzájárulását bármikor visszavonja. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.[2] A Hatóság kifejezetten jó gyakorlatnak tartja, ha az adatkezelő a hírlevélben

---

[1] A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:
a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.

[2] GDPR 7. cikk (3) bekezdés: Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

elhelyezett link segítségével megkönnyíti az érintetteknek, hogy a hírlevélküldési célú adatkezeléshez adott hozzájárulásukat visszavonhassák.

Ha az adatkezelés jogalapja az érintett hozzájárulása, abban az esetben a GDPR17. cikk (1) bekezdés b) pontja szerint az érintett jogosult arra, hogy az adatkezelő kérésére törölje a rá vonatkozó személyes adatokat, amennyiben az adatkezelésnek nincs más jogalapja.[3] (NAIH/2018/4018/3/V.)

b) Az adatkezelők a leggyakrabban közvetlen üzletszerzési célból küldenek hírlevelet az érintetteknek. Ebben az esetben az adatkezelés célja nem a hírlevélküldés, hanem a közvetlen üzletszerzés, amely adatkezelések vonatkozásában a GDPR speciális szabályokat tartalmaz.

A közvetlen üzletszerzési célú adatkezelések jogalapjaként az érintettek hozzájárulása, valamint az adatkezelő jogos érdeke[4] szolgálhat, amennyiben az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait. Ilyen jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Így például a személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.[5]

Ha az adatkezelés jogalapjául a GDPR 6. cikk (1) bekezdés f) pontja szolgál, az érintettet megilleti a tiltakozás joga. Az érintett tiltakozása esetén az adatkezelő a személyes adatokat nem kezelheti tovább. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ehhez nem kell semmilyen, a saját helyzetével kapcsolatos okot megjelölnie. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők,[6] és azokat az adatkezelőnek törölnie kell.[7]

---

[3] GDPR 17. cikk (1) bekezdés b) pont: Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll: az érintett visszavonja a 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja.

[4] GDPR 6. cikk (1) bekezdés f) pont: A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül: az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

[5] GDPR (47) preambulumbekezdés

[6] GDPR 21. cikk (1)-(3) bekezdés

[7] GDPR 17. cikk (1) bekezdés c) pont: az érintett a 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen.

7. „A GDPR Európán kívüli hatálya, figyelemmel az EvaGlawischnig-Piesczek ügyre (globális törlés előírhatósága), illetve az EUB döntése a CNIL-Google büntetésről (a "felejtés joga" csak Európában alkalmazandó).”

A GDPR extraterritoriális hatályát az EUB döntése nem érinti: a C-507/17 sz. Google vs. CNIL ügyben hozott döntés alapján[8] a GDPR alkalmazandó, ha vagy adatkezelő/adatfeldolgozó tevékenységi helye, vagy az érintett tartózkodási helye az Európai Gazdasági Térségben található. Az EUB csak azt mondta ki, hogy a jogkövetkezmények globális hatálya nem automatikus.

8. „A köztulajdonban álló gazdasági társaságokat érintő adatkezelési szabályok megegyeznek-e a tulajdonosra vonatkozó szabályokkal?”

A GDPR valamennyi jogi személy és természetes személy adatkezelőre alkalmazandó, kivéve egyes speciálisan nevesített adatkezelési tevékenységeket (nemzetbiztonság, honvédelem, bűnüldöző szervek, EU intézmények). Az, hogy egy adatkezelőnek ki a tulajdonosa önmagában nem bír jelentőséggel ezen szempontból. Például a 6. cikk (1) e) pont szerinti jogalap alkalmazásnál van jelentősége annak, hogy az adatkezelő maga (nem a tulajdonosa) közhatalmi szerv-e.

9. „Törlési kötelezettség teljesítése: az adatbázisból történő törlés megtörténte milyen módszerrel igazolható, mit vizsgál a Hatóság ennek körében egy esetleges eljárásban?”

Ha olyan rendszert használ az adatkezelő, amely pl. naplózza az ilyen műveleteket, akkor a vonatkozó naplóbejegyzés is megküldendő, vagy egyéb objektív bizonyíték szükséges az adott adatkezeléstől függően. Ezen felül az adatkezelő törvényes képviselőjének írásbeli nyilatkozata is bizonyító erővel rendelkezik, amelyben büntetőjogi felelőssége tudatában nyilatkozik a törlés teljesüléséről és annak idejéről.

10. „A különböző hatósági illetve egyéb szervek (szabálysértési hatóság, gyermekjóléti szolgálat, stb.) adatigényléseinek jogi alapja értelmezése és teljesíthetőségének feltételei, korlátjai?”

---

[8] C-507/17. 74. pont: A személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv 12. cikkének b) pontját és 14. cikke első bekezdésének a) pontját, valamint 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, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet) 17. cikkének (1) bekezdését úgy kell értelmezni, hogy a keresőmotor működtetője a link törlése iránti kérelem e rendelkezések alapján történő teljesítésekor e törlést nem köteles a keresőmotorjának valamennyi változatán elvégezni, hanem e törlést a keresőmotor tagállamok szerinti változataira köteles alkalmazni, szükség esetén olyan intézkedésekkel együtt, amelyek megfelelnek valamennyi jogszabályi előírásnak, és amelyek révén ténylegesen megakadályozhatók a tagállamok internethasználói abban, vagy legalábbis határozottan eltántoríthatók attól, hogy az érintett személy neve alapján a tagállamok valamelyikében végzett keresés eredményeként megjelenített találati lista révén hozzáférjenek a kérelem tárgyát képező linkekhez.

A hatóságok a jogszabályban megjelölt feladataik elvégzéséhez szükséges adatokat kérhetik, amely adott tevékenységenként eltérő lehet. Amennyiben megfelelő indokolás nélkül olyan személyes adatokat kér egy hatóság, amely nem lehet szükséges az eljárásához, akkor jogorvoslat kezdeményezhető az azt előíró döntéssel szemben az arra vonatkozó szabályok szerint.

11. „Adatkezelő vagy adatfeldolgozó, szükséges-e adatfeldolgozási szerződés?”

Amennyiben bármely személyes adatot kezelnek, azt vagy az adatkezelő vagy az adatfeldolgozó teheti meg. Személyes adat minden olyan adat, amely természetes személyhez köthető bárki, akár egy másik adatkezelő által (az álnevesített adat is) kifejezetten személyes adat a GDPR 4. cikk 5. pontja alapján, ezt a jellegét önmagában a személyes adat továbbítása nem módosítja. A személyes adatként történő minősüléshez nem szükséges az, hogy az adott adatkezelő vagy adatfeldolgozó birtokában legyen annak a többletinformációnak, amellyel az érintettek újra azonosíthatóak az álnevesített adatok alapján, elegendő, ha ezek az adatok bármely, az adatkezelőtől / adatfeldolgozótól különböző személy rendelkezésére áll.

Mindazon személyek, akik akár az adatkezelés céljának akár annak eszközeinek meghatározásában döntési joggal, beleszólással bírnak adatkezelőnek minősülnek. Ha egyvalaki jogosult dönteni ezekről a kérdésekről, akkor egy adatkezelő van, ha többen akkor közös adatkezelés valósul meg. Közös adatkezelő lehet például két önkormányzati fenntartású intézmény, ha írásbeli megállapodásuk alapján egyes adatkezelési feladatokat az egyikük végez mindkettejük helyett, de ennek feltételeit közösen állapították meg.

Aki a fenti feltételnek nem felel meg de az adatkezelő számára bármely műveletet végez a személyes adatokon, az adatfeldolgozó, és a GDPR alapján kötelező vele olyan megállapodás kötése (vagy a szerződésébe ezen feltételek egyértelmű belefoglalása külön pontban), amely a GDPR 28. cikk (3) bekezdése szerinti minimum elemeket tartalmazza. Az adatfeldolgozó (például garanciális javítást végző technikus cég) alkalmazottai nem önálló adatfeldolgozók, az ő tevékenységükért a munkáltatójuk felel.

12. „Megvásárolt adatbázis esetén van-e egy általános idő, amíg személyes adatok kezelhetők?”

Nincs általánosan alkalmazható időtartam, az adott adatkezelési cél és körülmények alapján határozható meg, hogy a cél eléréséhez mennyi ideig szükséges az adatkezelés. A GDPR alapján mind az eladónak mind a vevőnek rendelkeznie kell jogszerű, konkrét adatkezelési céllal és jogalappal az adatbázis átadásához. A GDPR (47) preambulumbekezdése alapján, ha az átvevőnek eddig semmilyen közvetlen kapcsolata nem volt az érintettek mindegyikével, akkor a jogos érdek jogalap nem lesz alkalmazható minden érintettel szemben, ahhoz önálló jogalap szükséges.

13. „GDPR 6. cikk (1) e) pontjában megjelölt közérdekű és közhatalom jogosítvány gyakorlásának keretében végzett adatkezelések elhatárolása”

A magyar tagállami jogszabályok nem különböztetik meg a két kategóriát a GDPR 6. cikk (1) e) ponton belül. Az Infotv. 5. § (3) bekezdése is közös követelményeket fogalmaz meg rájuk. Nincs magyar tagállami jogszabály, amely kifejezetten meghatározná a közhatalmi jogosítvány gyakorlására jogosult szerv fogalmát. Általános jogértelmezéssel olyan szervet jelent, amelyet

jogszabály feljogosít jogilag kötelező erejű intézkedések megtételére, jogok és kötelezettségek meghatározására. Példálódzó, iránymutató felsorolást tartalmaz az általános forgalmi adóról szóló 2007. évi CXXVII. törvény 7. § (2) bekezdése. Ennek alapján főszabály szerint közhatalmi tevékenység különösen a jogszabály-alkotási, az igazságszolgáltatási, az ügyészi, a védelmi, a rendvédelmi, a külügyi és igazságügyi igazgatási, a közigazgatási jogalkalmazói, a hatósági ellenőrzési és pénzügyi ellenőrzési, a törvényességi felügyeleti és ellenőrzési, az államháztartási, európai uniós és egyéb nemzetközi támogatás elosztásáról való döntési tevékenység.

14. „Rendeletalkotás során, nem egyértelmű felhatalmazás esetén az adatkezelésre vonatkozó szabályok meghatározása milyen mélységű lehet?”

Magyarország Alaptörvényének I. cikk (3) bekezdése alapján az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Ez alapján vagy az adatkezelést magát, vagy az adatkezelést szükségessé tevő közérdekű vagy közhatalmi tevékenységet közvetlenül hatályos uniós jogszabály, vagy magyar törvény kell meghatározza Magyarországon. Az Infotv. 5. § (3) bekezdése alapján kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve (törvényi felhatalmazás keretében kiadott) önkormányzati rendelet határozza meg. Rendeletek csak a fenti alapvető feltételeken túli, az a kötelező adatkezelés végrehajtásához szükséges és arányos adatkezelési feltételeket írhatják elő, szükség esetén megfelelő adatvédelmi hatásvizsgálat alapján. A rendelet helyettesítheti például az adatfeldolgozói szerződésen rendezendő, az Infotv. 5. § (3) bekezdésben nem említett feltételeit, mivel a GDPR 28. cikk (3) bekezdés szerinti „más jogi aktus” feltételeit teljesíti.

15. „A polgári törvénykönyvről szóló 2013. évi V. törvény (Ptk.) képmáshoz és hangfelvételvételhez való jog hogyan viszonyul a GDPR-hoz, annak adatkezelési jogalapjaihoz?”

A GDPR 23. cikke alapján az érintetti jogok korlátozhatóak, ha az arányos és szükséges egy demokratikus társadalomban. Így például a Ptk. tömegfelvételekre vonatkozó könnyítő rendelkezése is ilyen tagállami eltérés. A Ptk-ban írt könnyítések csak bizonyos feltételek mellett alkalmazhatóak és nem értelmezhetőek kiterjesztően. Ahol a GDPR nem enged eltérést, ott a Ptk. helyett a GDPR rendelkezései alkalmazandóak.

16. „A beléptető rendszer összeköthető-e a munkaügyi nyilvántartással, milyen jogalapot kell alkalmazni ebben az esetben?”

Igen, összeköthető, de tekintettel a két eltérő célú adatkezelésre, el kell különülnie a két adatbázisnak egymástól. A jogalap attól függően alakul, hogy milyen munkáltatóról van szó. Közhatalmat gyakorló, illetve közfeladatot ellátó szerveknél az általános adatvédelmi rendelet 6. cikk (1) bekezdés e) pontja, más munkáltatók esetén az általános adatvédelmi rendelet 6. cikk (1) bekezdés f) pontja lehet megfelelő jogalap. Az eszköz különböző adatkezelési célokra történő alkalmazásáról, az azok jogalapjához kötődő érintetti jogok gyakorlásának lehetőségeiről az érintettet a GDPR 12-13. cikke és az Adatvédelmi Irányelv 29-es cikke alapján létrehozott

Adatvédelmi Munkacsoport átláthatóságról szóló iránymutatás (https://naih.hu/files/wp260rev01_hu.pdf) szerint tájékoztatni szükséges.

17. „Használhatók-e a munkavállaló biometrikus adata (ujjlenyomat) a belső munkaügyi folyamatok keretében az alábbi esetekben: fokozott biztonságú elektronikus aláírás beszerzése erre szolgáló program segítségével munkaügyi anyagok aláírásánál. Például munkaszerződés, átadás-átvételi jegyzőkönyv, vagy szabályzat tudomásulvételi nyilatkozat aláírása elektronikusan. Az adatkezelés jogalapja a munkáltató jogos érdeke lenne és érdekmérlegelési tesztet alkalmaznánk."

Munkaviszonyban a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) 11. § (1)-(2) bekezdése meghatároz bizonyos eseteket, érdekeket – például a munkavállalók vagy mások élete, testi épsége vagy egészsége súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélye áll fenn a munkahelyen; vagy a munkáltató mérgező vagy veszélyes vegyi vagy biológiai anyagokat tárol; vagy a munkáltató a Büntető Törvénykönyvről szóló 2012. évi C. törvény szerint legalább különösen nagy vagyoni értékű vagyontárgyakat őriz –, amelyek jogszerűek lehetnek és amennyiben a szükségesség-arányosság követelménye teljesül, adott esetben jogszerűen kezelhetők a munkavállalók biometrikus adatai, ha az adatkezelés célja jogszerű és van megfelelő jogalap, jelen esetben a jogos érdek jogalapja. Az Mt. 11. § (1) bekezdés b) pontjában megjelölt törvényben védett jelentős érdekek a „különösen" szóból következően ugyanakkor csupán példaként értelmezendők, ezeken kívül a Hatóság adott esetben más törvényben védett érdekeket is elfogadhat, amennyiben az érdekmérlegelés során az adatkezelés szükségessége és arányossága igazolt.

Amennyiben a munkáltató közhatalmat gyakorló vagy közfeladatot ellátó szerv, az adatkezelésre az általános adatvédelmi rendelet 6. cikk (1) bekezdés e) pontja teremthet jogalapot.

Pusztán kényelmi szempontok nem alapozzák meg, hogy biometrikus adatokat kezeljen az adatkezelő, továbbá amennyiben van más alternatív és kisebb jogkorlátozással járó módszer, akkor azt kell alkalmazni a biometrikus adatkezelést végző rendszerrel szemben.

18. Munkahelyen történő beléptetéssel és kamerás megfigyeléssel kapcsolatos kérdések (pl. lehet-e kamerákat alkalmazni munkavállalók magatartásának és munkarenddel összefüggő ellenőrzése végett?)

Az Mt. 11/A. § (1) bekezdése értelmében a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja.

Ugyanakkor figyelembe veendő a tisztességes adatkezelés elve, mivel a tisztességtelen adatkezelési magatartás az érintetteket nemcsak a személyes adatok védelméhez, de az emberi méltósághoz fűződő jogában is súlyosan sértheti. Ebből kifolyólag a kamerás megfigyelés abszolút korlátját jelenti az emberi méltóság tiszteletben tartása, ezért kamerákat nem lehet működtetni a munkavállalók és az általuk végzett tevékenység állandó jellegű megfigyelésére. Jogellenesnek és tisztességtelennek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása, amelynek célja a munkavállalók munkahelyi viselkedésének a befolyásolása, a munkavállalók kamerákkal történő folyamatos megfigyelése, ellenőrzése. Az Alkotmánybíróság a 36/2005. számú – a Hatóság által továbbra is irányadónak tekintett - határozatában kimondta, hogy *„az elektronikus úton történő*

megfigyelés tehát alkalmas arra, hogy a magánszférába behatoljon, intim (szenzitív) élethelyzeteket rögzítsen akár olyképpen, hogy az érintett nem is tud a felvételről, vagy nincs abban a helyzetben, hogy mérlegelhesse az ilyen felvételek megengedhetőségét és azok következményeit. Az így végzett megfigyelés a magánélethez való jog sérelmén túl – szélesebb és mélyebb értelemben – az emberi méltósághoz való jogot általában is érintheti. A magánszféra lényegi fogalmi eleme éppen az, hogy az érintett akarata ellenére mások oda ne hatolhassanak be, illetőleg be se tekinthessenek. Ha a nem kívánt betekintés mégis megtörténik, akkor nemcsak önmagában a magánélethez való jog, hanem az emberi méltóság körébe tartozó egyéb jogosultsági elemek, mint pl. az önrendelkezési szabadság vagy a testi-személyi integritáshoz való jog is sérülhet."

Munkavállaló kamerás megfigyelésével összefüggő ügyben a Hatóság az alábbi linken elérhető határozatot hozta: https://naih.hu/files/NAIH_2019_2466_hatarozat.pdf

19. „A vagyonőr által alkalmazható elektronikus megfigyelőrendszer a 2005. évi CXXXIII. tv. 30.§ (1) bek. szerint: magánterület és a magánterület közforgalom számára megnyitott részének elhatárolása a kamerarendszer alkalmazása szempontjából."

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: Szvtv.) 30. § (2) bekezdése szerint a vagyonőr elektronikus megfigyelőrendszert kizárólag magánterületen alkalmazhat. A Hatóság álláspontja szerint a lényeg az, hogy közterület nem figyelhető meg – szűk körtől eltekintve – magánterületen alkalmazható elektronikus megfigyelőrendszer, annak a közönség számára nyilvános részén is.

20. „A NAIH kap-e felkérést az új törvények adatvédelmi felülvizsgálatára, az ellentmondások kiküszöbölésére?"

Az Infotv. 38. § (4) bekezdés a) pontja szerint a Hatóság javaslatot tehet a személyes adatok kezelését, valamint a közérdekű adatok és a közérdekből nyilvános adatok megismerését érintő jogszabályok megalkotására, illetve módosítására, véleményezi a feladatkörét érintő jogszabályok tervezetét. Ez - a kérdésben megfogalmazottaktól eltérően – nem utólagos, hanem előzetes véleményalkotást jelent, még a jogszabály elfogadása és hatálybalépése előtt. A Hatóság ezen hatáskörében rendszeresen kap felkérést az egyes minisztériumoktól előkészítés alatt álló jogszabály-tervezetek véleményezésére, elsősorban a személyes adatok védelmét és a közérdekű adatok nyilvánosságát érintő tervezetek körében. A jogszabályok utólagos felülvizsgálata a Hatóságnál nem formalizált módon zajlik: a Hatóság munkája során kerülnek elő olyan problémák, amelyek forrása esetleg valamely jogszabály téves jogalkalmazói értelmezése, ami esetleg a kevésbé pontos kodifikáció eredménye, és a hatósági munka során találkozunk olyan esettel is, amikor ellentmondás fedezhető fel két jogszabály között. Ezeket az eseteket az Infotv.-ben biztosított hatáskörünk alapján jelezzük a jogszabály előkészítéséért felelős tárca felé, és egyben javaslatot is teszünk a helyesnek tartott jogalkotásra.

21. „A jövőben mely területeken várható az ágazati jogszabályok GDPR-hoz igazítása? A 2019. évi salátatörvény csak minimális mértékben fedte le a problémás területeket. Pl. szociális ágazati jogszabályok…"

Az előző kérdéshez is kapcsolódóan megválaszolva: mivel az új jogszabályok előkészítéséért az egyes tárcák a felelősek, ezért konkrét választ a Hatóság nem tud adni a jogalkotás várható jövőbeni

irányáról. Mindenesetre amely szakigazgatási területen a hatósági munka során hiányossággal találkozunk, azt következetesen jelezni szoktuk a jogalkotás előkészítéséért felelős tárcának. A tárcákkal való együttműködésünk ebből a szempontból produktívnak nevezhető.

22. „Mik a tanúsítás végrehajtásának követelményei?”

A GDPR és az Infotv. kapcsolódó rendelkezései mellett az Európai Adatvédelmi Testület 1/2018. számú iránymutatása [https://naih.hu/files/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_hu.pdf] és a Hatóság 2018. évi beszámolója adhat bővebb iránymutatást a témában.

23. „Mikorra várható a tanúsítási mechanizmus bevezetése, a Hatóság maga, vagy tanúsító szervezetek révén kívánja ezt a feladatot ellátni?”

Tanúsítási tevékenységet az Európai Adatvédelmi Testület 1/2018. számú iránymutatása szerinti szempontok figyelembevételével az Infotv. 69. § rendelkezései alapján maga a Hatóság is végezhet, illetve arra a Hatóság 2018. évi beszámolójában kifejtett engedélyezési eljárást követően bármely más akkreditált szervezet is jogosult lehet. A tanúsító szervezetek akkreditációjához szükséges kiegészítő szempontrendszert az iránymutatásban foglaltak alapján a Hatóság állítja össze, majd azt az Európai Adatvédelmi Testület elé terjeszti.

24. Adatvédelmi tisztviselőhöz kapcsolódó, a videós előadásban nem vizsgált kérdések

Az általános adatvédelmi rendelet szabályait összefoglalva a Hatóság honlapján elérhető egy tájékoztató, mely tartalmazza, mely esetekben kell adatvédelmi tisztviselőt kinevezni, illetve milyen esetekben állhat fenn összeférhetetlenség: https://naih.hu/files/Tajekoztato-adatvdedelmi-tisztviselo-kinevezeserol-2018-09-19.pdf

25. Okmánymásoláshoz kapcsolódóan feltett kérdések

Az Mt. 10. § (1) és (3) bekezdése alapján a munkáltató a munkavállalótól olyan nyilatkozat megtételét vagy személyes adat közlését követelheti, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy e törvényből származó igény érvényesítése szempontjából lényeges. Ez alapján a munkáltató okirat bemutatását követelheti a munkavállalótól.

A hatályos jogszabályi rendelkezéseknek tehát az okmány bemutatása felel meg, a másolatok kezelése azonban nem felel meg sem a célhoz kötött adatkezelés, sem az adattakarékosság követelményének, amiatt sem, mivel az okmányokon olyan személyes adatok is szerepelnek, amelyek a munkaviszony szempontjából nem szükségesek. A hatósági igazolványról készített másolat továbbá nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági okmánynak.

A Hatóság álláspontja szerint a szükségesség-arányosság szempontrendszere alapján az okmányokkal végzett jogszerű többletintézkedés lehet például az, ha a munkáltató ügyintézője egy nyilatkozat kitöltését kéri az érintettől arról, hogy mely hatósági okmányát mutatta be. Továbbá alkalmazható az úgynevezett „négy szem elve” is, amikor egy másik ügyintéző vagy az ügyintéző felettese is megtekinti az érintett által bemutatott okmányt, és ő is megerősíti a rögzített adatok

pontosságát. Kevésbé korlátozza a magánszférát egy feljegyzés készítése vagy egy nyilatkozat kitöltése, mint az okmányok másolása. A Hatóság álláspontja szerint a fénykép vagy másolat készítése főszabály szerint nem tekinthető a magánszféra arányos korlátozásának más, hasonlóan hatékony intézkedésekhez képest. A Hatóság megjegyzi, hogy kényelmi szempontok vagy „gyorsabb ügyintézés” szintén nem indokolhatják a másolat készítését.

A Hatóság abban az esetben fogadja el másolatok készítését, ha a munkáltató mint adatkezelő olyan gyakorlatot alakít ki, amelynek során kizárólag azon adatokról készít másolatot, amelynek kezelésére egyébként jogosult. Ebben az esetben az okmányon található adat lemásolása ugyan adatkezelési művelet, de nem új adatkezelési cél az adatgyűjtés eredeti céljához képest, hanem az eredeti adatkezelési céllal és ahhoz kapcsolódó jogalappal történő adatgyűjtés egy olyan módja, amely egyébként segít az adatok pontosságának biztosításában.