OAHSZD/10-1/2026

Az Országos Atomenergia Hivatal
8/2026. (VII.1.) elnöki utasítása
az Országos Atomenergia Hivatal Adatvédelmi és Adatbiztonsági Szabályzatáról

Az atomenergiáról szóló 1996. évi CXVI. törvény 6/J. § (1) bekezdés d) pontjában kapott felhatalmazás alapján, az Országos Atomenergia Hivatal Szervezeti és Működési Szabályzatáról szóló 1/2022. (III.10.) OAH utasítás 7. § (2) bekezdés 18. pontjában meghatározott hatáskörömben eljárva - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet 24. cikk (2) bekezdésében, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdésében foglaltak alapján - a következő utasítást adom ki:

1. § Az Országos Atomenergia Hivatal Adatvédelmi és Adatbiztonsági Szabályzatát az 1. mellékletben foglaltak szerint határozom meg.

2. § Az utasítás a közzétételét követő napon lép hatályba.

3. § Hatályát veszti az OAH Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 13/2021. főigazgatói utasítás.

.....
Kádár Andrea Beatrix
elnök

1. melléklet a 8/2026 (VII.1.) elnöki utasításhoz

AZ ORSZÁGOS ATOMENERGIA HIVATAL ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

I. Fejezet

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja

1. § Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: AASZ) célja, hogy biztosítsa az Országos Atomenergia Hivatal (a továbbiakban: OAH) által kezelt személyes adatok vonatkozásában az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, valamint meghatározza az OAH által vezetett, adatvédelemmel kapcsolatos nyilvántartások kezelésének rendjét.

2. § Az AASZ a 3. alcímben felsorolt jogszabályokban rögzített rendelkezésekkel együttesen értelmezendő és alkalmazandó.

2. Az AASZ hatálya

3. § (1) Az AASZ személyi hatálya kiterjed az OAH valamennyi szervezeti egységének foglalkoztatottjára.

(2) Az AASZ tárgyi hatálya kiterjed az OAH szervezeti egységeinél nyilvántartott valamennyi személyes adatra, a velük végzett adatkezelési műveletek teljes körére keletkezésük, felhasználásuk, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

3. Az AASZ jogszabályi alapja, kapcsolata a belső szabályzatokkal

3. § (1) Az AASZ jogszabályi alapját többek között:

a) az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR);
b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
c) a minősített adat védelméről szóló 2009. évi CLV. törvény,
d) az atomenergiáról szóló 1996. évi CXVI. törvény,
e) a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény,
f) a különleges jogállású szervekről és az általuk foglalkoztatottak jogállásáról szóló 2019. évi CVII törvény (a továbbiakban: Küt.)
g) a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény,

h) Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény,
i) köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény,
j) az államháztartásról szóló 2011. évi CXCV. törvény,
k) a számvitelről szóló 2000. évi C. törvény,
l) az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény,
m) a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: Szvtv.) rendelkezései biztosítják.

(2) Az AASZ szorosan kapcsolódik az OAH alábbi belső szabályozó dokumentumaihoz:

a) Az Országos Atomenergia Hivatal elnökének 1/2022. (III. 10.) OAH utasítása az Országos Atomenergia Hivatal Szervezeti és Működési Szabályzatáról (a továbbiakban: SzMSz)
b) SZ-09 Szabályzat a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről, valamint egyes adatok közzétételéről,
c) SZ-02 Informatikai Biztonsági Szabályzat (a továbbiakban: Informatikai Biztonsági Szabályzat),
d) SZ-17 Az OAH Szabályzata az elektronikus megfigyelőrendszer üzemeltetéséről és az ezzel kapcsolatos adatkezelésről,
e) SZ-06 Házirend,
f) Az Országos Atomenergia Hivatal elnökének 2/2023. (XII.28.) OAH utasítása az Országos Atomenergia Hivatal Közszolgálati Szabályzatáról,
g) Az Országos Atomenergia Hivatal elnökének 1/2024. (I.11.) OAH utasítása az Országos Atomenergia Hivatal minősített adatok védelmére vonatkozó biztonsági szabályzatának kiadásáról,
h) Az Országos Atomenergia Hivatal elnökének 2/2024. (I.25.) OAH utasítása az Országos Atomenergia Hivatal TÜK 2 SZT PC1 és SZT PC2 üzemeltetés biztonsági szabályzatáról,
i) Az Országos Atomenergia Hivatal 5/2024. (I.22.) elnöki utasítása az Országos Atomenergia Hivatal Munkavédelmi Szabályzatáról,
j) Az Országos Atomenergia Hivatal elnökének 2/2025. (XII.19.) OAH utasítása az Országos Atomenergia Hivatal Iratkezelési Szabályzatáról (a továbbiakban: Iratkezelési Szabályzat).

5. § Az AASZ alkalmazása során használatos alapfogalmak értelmezését az 1. függelék tartalmazza.

4. A személyes adatok kezelésére vonatkozó alapelvek

6. § A személyes adatok kezelésére az alábbi alapelvek irányadók a GDPR 5. cikke alapján:

a) a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás könnyen hozzáférhető és közérthető legyen, ennek biztosítása érdekében az OAH tájékoztatót helyez el a honlapján („jogszerűség, tisztességes eljárás és átláthatóság”);

b) a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, a személyes adatok nem kezelhetők az adatkezelési célokkal össze nem egyeztethető módon; („célhoz kötöttség”);

c) az adatkezelés során az adatkezelés céljai szempontjából megfelelőek és relevánsak, kezelésüknek az adatkezelés célja szempontjából a szükségesre kell korlátozódniuk („adattakarékosság”);

d) pontosságát és naprakészségét biztosítani kell, ezért az OAH-nak minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; (korlátozott tárolhatóság”);

f) kezelését az OAH oly módon végzi, hogy megfelelő technikai és/vagy szervezési intézkedéseket alkalmaz annak érdekében, hogy a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelem is biztosítva legyen („integritás és bizalmas jelleg”).

g) az OAH, mint adatkezelő felelős az a) - f) pontoknak való megfelelésért, továbbá képesnek kell lennie a megfelelés igazolására („elszámoltathatóság”).

II. Fejezet

JOGSZERŰ ADATKEZELÉS ÉS AZ ÉRINTETTI JOGOSULTSÁGOK

5. Az adatkezelés jogalapja és általános feltételei

7. § (1) Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból kezelhető. A 8. §-ban felsorolt feltételek legalább egyikének a teljesülése biztosítja az adatkezelés kellő jogalapját, jogszerűségét.

8. § (1) Az adatkezelés jogalapja lehet:

a) az érintett hozzájárulását adta személyes adatainak egy, vagy több konkrét célból történő a kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az OAH-ra vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett, vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű, vagy az OAH-ra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés azért történik, mert az OAH-nak vagy egy harmadik félnek jogos érdeke fűződik hozzá, kivéve, ha ezt az érdeket megelőzik az érintett személy olyan érdekei vagy alapvető jogai és szabadságai, amelyek a személyes adatok védelmét indokolják, különösen, ha ez az érintett személy gyermek.

(2) Az adatkezelés célját az a-f) pontokban rögzített adatkezelési jogalapok egyikére hivatkozással kell meghatározni, illetve az e) pontban említett adatkezelés tekintetében annak szükségesnek kell lennie valamely közérdekű feladat, vagy az OAH-ra ruházott közhatalmi jogosítvány gyakorlása során végzett feladat végrehajtásához.

(3) a) A GDPR 6. cikk (1) bekezdés c) és e) pontjában foglaltak alapján meghatározott adatkezelés (a továbbiakban: kötelező adatkezelés) esetén a kezelendő adatok fajtáit, az adatkezelés célját és

feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, az adatkezelés időtartamát, vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény határozza meg.
b) Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az OAH az adatkezelés megkezdését követően legalább háromévente felülvizsgálja, hogy az általa, illetve megbízásából, vagy rendelkezése alapján eljáró adatfeldolgozó adatkezelése szükséges-e az adatkezelés céljának a megvalósulásához.

(4) A Küt. alapján az OAH a köztisztviselőkre vonatkozó adatokat statisztikai célból – személyazonosításra alkalmatlan módon – felhasználhatja, illetve e célból továbbíthatja. Ezen adatkezelés jogalapja jogi kötelezettség teljesítése, illetve közérdekű feladat végrehajtása.

9. § (1) Különleges adat kezelése tilos.

(2) Az (1) bekezdésben foglaltaktól eltérően különleges adat abban az esetben kezelhető, ha:

a) ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli;

b) az érintett kifejezetten hozzájárult a rá vonatkozó különleges adat egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós, vagy a magyar jog úgy rendelkezik, hogy az adatkezelési tilalom nem oldható fel az érintett hozzájárulásával;

c) az adatkezelés az OAH-nak vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha azt az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező európai uniós vagy magyar jog ezt lehetővé teszi;

d) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;

e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;

f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;

g) az adatkezelés jelentős közérdek miatt szükséges, európai uniós jog vagy magyar jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a foglalkoztatott munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások

irányítása érdekében szükséges, uniós vagy magyar jog alapján vagy egészségügyi szolgáltatóval kötött szerződés értelmében, továbbá a GDPR-ban említett feltételekre és garanciákra figyelemmel;

i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy magyar jog alapján, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

j) az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy magyar jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

(3) A különleges adatok kezelése esetén az OAH, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó megfelelő műszaki és szervezési intézkedésekkel biztosítja, hogy az adatkezelési műveletek végzése során a különleges adatokhoz kizárólag az rendelkezzen hozzáféréssel, akinek az adatkezelési művelettel összefüggő feladata ellátásához feltétlenül szükséges.

(4) A büntetőeljárással kapcsolatos adatok kezelésére a Küt.-ben foglalt eltérő szabályok az irányadók.

10. § Ha az adatkezelést az OAH nevében más végzi, kizárólag olyan adatfeldolgozó vehető igénybe, aki, vagy amely megfelelő garanciákat nyújt az adatkezelés GDPR-ban rögzített követelményeinek érvényesüléséhez és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy a magyar jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az OAH-val szemben.

11. § (1) A közös adatkezelés akkor valósul meg, ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg.

(2) A közös adatkezelők az adatkezelés tekintetében az érintettekkel történő kapcsolattartásra kapcsolattartót jelölnek ki. A kapcsolattartó kijelölése nem érinti az adatkezelők felelősségét.

(3) A közös adatkezelést valamennyi adatkezelő a közöttük létrejött megállapodás szerint végzi, a felelősségük a megállapodásban meghatározott feladatmegosztásnak megfelelő. A megállapodás lényegét az érintettekkel ismertetni kell.

(4) A közös adatkezelői megállapodás, illetve a közös adatkezelés ténye az érintett számára a jogai gyakorlása vonatkozásában nem lehet terhesebb. Erre tekintettel az érintett bármely adatkezelő felé joghatályosan megteheti mindazt, illetve valamennyi törvényes jogával ugyanúgy élhet, mintha egy adatkezelő végezné a személyes adatok kezelését.

6. Az adattovábbítás feltételei

12. § (1) Az adattovábbítást megelőzően az OAH megvizsgálja a továbbítandó személyes adatok pontosságát, teljességét és naprakészségét. Az adattovábbítás akkor minősül jogszerűnek, ha a személyes adatot kezelő szervezeti egység, vagy személy jogosult annak továbbítására; az adattovábbítás címzettje pedig rendelkezik az adat kezeléséhez szükséges jogalappal, vagy az érintett írásbeli – a vonatkozó jogszabályi előírásoknak megfelelő tartalmú – hozzájárulásával és a továbbítandó adatok köre az alkalmazandó jogszabályi követelményekre figyelemmel az adatkezelés céljához szükséges körre korlátozódik.

(2) Személyes adatot az OAH harmadik országban, továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére – a közvetett adattovábbítást is ideértve – akkor továbbíthat, ha

a) a nemzetközi adattovábbításhoz az érintett kifejezetten hozzájárult, vagy

b) a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, valamint

ba) annak során az adatkezelésnek a 6. alcímben rögzített feltételei teljesülnek, és

bb) a harmadik országban, illetve a nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó tekintetében a továbbított személyes adatok megfelelő szintű védelme biztosított, vagy

c) a nemzetközi adattovábbítás

ca) az érintett vagy más személy létfontosságú érdekeinek védelme érdekében szükséges,

cb) valamely EGT-állam vagy harmadik ország közbiztonságát közvetlenül és súlyosan fenyegető veszély elhárítása érdekében szükséges,

cc) egyedi ügyben, eseti jelleggel az OAH által végzett vizsgálatok vagy eljárások hatékony és eredményes lefolytatása érdekében szükséges, és az nem jár az érintett alapvető jogainak aránytalan korlátozásával,

cd) egyedi ügyben, eseti jelleggel az érintett vagy más jogi igényeinek előterjesztése, érvényesítése, illetve védelme érdekében szükséges, és az nem jár az érintett jogainak aránytalan korlátozásával.

(3) Olyan adatkezelés esetén, amelynél számolni kell külföldre irányuló adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni.

(4) Az adattovábbítás papír alapon vagy elektronikus úton történhet.

(5) Az OAH szervezetén belül a kezelt személyes adat - a feladat elvégzéséhez szükséges mértékben és ideig - csak a feladattal érintett szervezeti egységhez továbbítható, feltéve, hogy a személyes adatok megismerése nélkül a feladatot érdemben végrehajtani nem lehet. Az OAH szervezetén belül a különböző célú adatkezelések csak törvényes cél érdekében, indokolt esetben, ideiglenesen kapcsolhatók össze.

(6) Az OAH a közszolgálati jogviszonyból származó kötelezettségek teljesítése céljából a köztisztviselő személyes adatait az adatfeldolgozó részére átadhatja.

(7) Az adattovábbítás minden esetben célhoz kötött, és arról az érintettet előzetesen tájékoztatni kell**.**

7. Az érintett jogai

13. § (1) Az OAH és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában az érintett az alábbiakra jogosult:

a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (előzetes tájékozódáshoz való jog),

b) kérelmére személyes adatai és az azok kezelésével összefüggő információk rendelkezésre bocsátására (hozzáféréshez való jog),

c) kérelmére személyes adatai helyesbítésére, illetve kiegészítésére (helyesbítéshez való jog),

d) kérelmére személyes adatai kezelésének a korlátozására (az adatkezelés korlátozásához való jog),

e) kérelmére személyes adatai törlésére (törléshez való jog),

f) az érintettre vonatkozó, az OAH rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az OAH, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált. Az adathordozhatósághoz való jog nem sértheti a törléshez való jogot („az elfeledtetéshez való jogot”). Az adathordozhatóság nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az OAH-ra ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges. Az adathordozhatósághoz való jog nem érintheti hátrányosan mások jogait és szabadságait (adathordozhatósághoz való jog).

(2) Az OAH az érintett jogai érvényesülésének elősegítése érdekében megfelelő műszaki és szervezési intézkedéseket tesz és az érintettől érkező kérelmeket az alábbi módon bírálja el:

a) az érintettől érkező kérelem esetén az adatok kezelését végző szervezeti egység vezetője felveszi a kapcsolatot az adatvédelmi tisztviselővel, akivel közösen javaslatot tesznek a kérelemre adandó válaszra. A választ az OAH elnökének jóváhagyását követően küldik meg az érintettnek.

b) az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb idő alatt, de legfeljebb huszonöt napon belül elbírálja és döntéséről az érintettet írásban, vagy elektronikus úton értesíti.

(3) Az OAH a 13. § (1) bekezdésben foglalt jogok érvényesülésével kapcsolatban meghatározott feladatait – törvényben rögzített kivétellel - ingyenesen látja el.

(4) Ha megalapozottan feltehető, hogy a 13. § (1) bekezdés b) - e) pontjában meghatározott jogok érvényesítése iránt kérelmet benyújtó személy az érintettel nem azonos személy, az OAH a kérelmet az azt benyújtó személy személyazonosságának hitelt érdemlő igazolását követően teljesíti.

(5) A 13. § (1) bekezdés a) pont szerinti előzetes tájékoztatás az OAH-ban az Szvtv. szabályai alapján működő elektronikus megfigyelőrendszerrel kapcsolatban ki kell, hogy terjedjen:

a) az elektronikus megfigyelő rendszer kamerái helyeire, illetőleg arra, hogy a kamerák mit rögzítenek;

b) az adatkezelő és az adatfeldolgozó személyére, illetőleg azon természetes személyek nevére, beosztására, akik a kamerák felvételeihez hozzáférhetnek.

(6) Ha az érintett jogai gyakorlásának korlátozásával vagy teljesítésének megtagadásával kapcsolatos döntést kell meghoznia az OAH-nak, a kérelemre adott válaszban tájékoztatni kell az érintettet a jogi, ténybeli indokokról, az őt megillető jogokról és a jogorvoslati lehetőségekről.

III. Fejezet

A FOGLALKOZTATÁSSAL ÖSSZEFÜGGŐ ADATKEZELÉSEK

14. § (1) Az OAH a köztisztviselők személyes adatait a közszolgálati jogviszony létesítésével, fenntartásával és megszüntetésével összefüggésben kezeli.

(2) Az adatkezelés a vonatkozó jogszabályok, különösen a Küt. rendelkezésein alapul.

(3) Amennyiben az OAH a büntetőeljárásról szóló törvény alapján tájékoztatást kap arról, hogy a köztisztviselővel szemben büntetőeljárás indult, jogosult kezelni:

a) a természetes személyazonosító adatokat,
b) a büntetőeljárás megindításának tényére vonatkozó adatot.

(4) Az adatkezelés időtartama:

a) legfeljebb 15 nap, vagy
b) munkáltatói intézkedés esetén az intézkedés meghozataláig.

(5) Az adatkezelés céljának megszűnését követően az adatokat haladéktalanul törölni kell.

(6) Az e § szerinti adatkezelések során keletkező dokumentumokat az Iratkezelési Szabályzat szerint kell kezelni.

IV. Fejezet

AZ OAH ADATVÉDELMI SZERVEZETE

8. Az adatvédelemért felelősök feladatai

15. § (1) Az OAH elnöke

a) kijelöli az adatvédelmi tisztviselőt, nevét és elérhetőségét közli a felügyeleti hatósággal, biztosítja a feladata elvégzéséhez szükséges feltételeket,

b) kiadja az AASZ-t,

c) felügyeli az adatvédelmi feladatok ellátását.

16. § (1) Az adatvédelmi tisztviselő közvetlenül az OAH elnökének tartozik felelősséggel, feladatai ellátása során önállóan jár el.

(2) Az adatvédelmi tisztviselő más feladatokat is elláthat, de csak akkor, ha e feladatokból nem fakad összeférhetetlenség.

(3) Az adatvédelmi tisztviselő feladatait részletesen a SzMSz 4. függelékének 2. pontja tartalmazza. Az adatvédelmi tisztviselő az ott meghatározott feladatait a GDPR 37–39. cikkeiben foglaltaknak megfelelően látja el.

17. § Az önálló szervezeti egységek vezetői

a) felelősek azért, hogy az általuk vezetett szervezeti egységnél az adatkezelés a vonatkozó jogszabályok és az AASZ rendelkezései szerint történjék;

b) gondoskodnak az általuk végzett adatkezelések belső adatvédelmi nyilvántartásba történő bejelentéséről, valamint a változások folyamatos átvezetéséről;

c) felelősek azért, hogy a szervezeti egység adatkezelési tevékenysége során az adatbiztonsági előírások maradéktalanul teljesüljenek;

d) gondoskodnak arról, hogy a személyes adatokhoz való hozzáférési jogosultságok naprakészek legyenek, különös tekintettel a belépő, távozó, vagy tartósan távollévő munkatársakra.

f) adatvédelemmel kapcsolatos problémák, adatvédelmi incidens gyanújának észlelése esetén írásban soron kívül tájékoztatják az Informatikai és Biztonsági Főosztályt és az adatvédelmi tisztviselőt.

18. § Az adatkezelést végző személy

a) tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért;

b) kezeli és megőrzi a feladata ellátása során birtokába került adatokat;

c) ügyel a nyilvántartások biztonságos kezelésére és tárolására;

d) gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz illetéktelen személy ne férhessen hozzá;

e) betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat;

f) részt vesz az adatkezeléssel, adatvédelemmel összefüggő szakmai képzéseken;

g) adatkezeléssel, adatvédelemmel kapcsolatos problémák, adatvédelmi incidens gyanújának észlelése esetén írásban soron kívül tájékoztatja a szervezeti egység vezetőjét, az és az adatvédelmi tisztviselőt.

V. Fejezet

A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK ÉRVÉNYESÜLÉSE AZ OAH-NÁL

9. Az adatkezelés kialakításával kapcsolatos kötelezettségek

19. § (1) A beépített adatvédelem érvényesítése elősegíti, hogy az adatkezelési folyamat során az adatvédelmi előírások betartása könnyen ellenőrizhető legyen.

(2) Az alapértelmezett adatvédelem elveinek megfelelően az OAH gondoskodik arról, hogy a személyes adatok védelmére vonatkozó szabályok, védelmi intézkedések és hozzáférési jogosultságok a lehető legszigorúbb adatvédelmi beállítások szerint kerüljenek meghatározásra és alkalmazásra.

(3) Az OAH elektronikus információs rendszereihez a hozzáférési jogosultságokat hierarchikusan, szintenként kell kialakítani. Az OAH valamennyi elektronikus információs rendszeréhez való hozzáférés szerepkör-alapon, a legkisebb jogosultság elvének megfelelően kerül kiosztásra. A hozzáférések igénylését, jóváhagyását, módosítását és visszavonását dokumentálni kell. A

hozzáférések rendszeres felülvizsgálata biztosított, valamint minden hozzáférési esemény naplózásra kerül.

10. A belső adatvédelmi nyilvántartás

20. § (1) A belső adatvédelmi nyilvántartás az OAH szervezeti egységeinél történő személyes adat kezelésekkel kapcsolatban az adatkezelési célok mentén, a GDPR 30. cikke által meghatározott tartalommal tartja nyilván legalább

a) az adatkezelés célját;

b) az adatok fajtáját és kezelésük jogalapját;

c) az érintettek körét;

d) az adat forrását;

e) az esetleges adattovábbítások fajtáját, címzettjét és a továbbítás jogalapját;

f) az egyes adatfajták törlésének határidejét;

g) az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét.

(2) A belső adatvédelmi nyilvántartás mintatáblázatát a 2. függelék tartalmazza, az adatvédelmi nyilvántartást az adatvédelmi tisztviselő kezeli és frissíti. Az adatvédelmi tisztviselő a hatályos adatvédelmi nyilvántartást az OAH zárt informatikai rendszerében tárolja.

11. Adatbiztonság

21. § (1) Az OAH a kezelésében lévő személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását azáltal biztosítja, hogy az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész., zárt, teljes körű és folytonos szervezési és technikai védelmi intézkedéseket alkalmaz. Ennek érdekében az OAH az alábbi technikai és szervezési intézkedéseket hajtja végre:

a) a tudomány és technológia mindenkori szintjének megfelelő, arányos és hatékony biztonsági intézkedéseket alkalmaz;

b) biztosítja, hogy fizikai vagy műszaki incidens esetén a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állása időben helyreállítható legyen;

c) az adatkezelés biztonságát szolgáló technikai és szervezési intézkedések hatékonyságának felmérésére és értékelésére szolgáló eljárások rendszeres tesztelését és értékelését elvégzi

(2) A biztonság sérüléséhez vezető minden kockázatot értékelni kell, amelyek a személyes adatok véletlen, vagy jogellenes megsemmisítéséből, elvesztéséből, módosításából, vagy a személyes adatokhoz történő jogosulatlan hozzáférésből származhatnak.

(3) Adatkarbantartást csak az erre felhatalmazott foglalkoztatott végezhet.

(4) Az adatbiztonság betartásáért a központi elektronikus információs rendszerek vonatkozásában az Informatikai Osztály vezetője, a nem központi elektronikus információs rendszerek vonatkozásában az adatfeldolgozást végző szervezeti egység vezetője a felelős.

22. § (1) Az adatokhoz hozzáférni jelszavas védelemmel és jogosultsági rendszer működtetésével lehet.

(2) Az elektronikus információs rendszerek üzemeltetését ellátó munkatársak a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják.

(3) A központi elektronikus információs rendszerek esetében a hozzáféréseket központi jogosultságkezelési rendszerben, szerepkör-alapon kell kezelni. A hozzáférések igénylése, jóváhagyása és kiosztása dokumentált folyamat mentén valósul meg, és rendszeres felülvizsgálat tárgyát képezi.

(4) Az egyedi alkalmazások lokális gépein a speciális adatfeldolgozó szoftver saját jelszó és jogosultsági rendszerét kell alkalmazni. A jelszavak használatáért, azok rendszeres változtatásáért és dokumentálásáért az adott szervezeti egység vezetője, vagy az adott rendszerhez tartozó adatgazda felelős.

(5) A központi rendszer és az egyedi rendszerek hozzáférési jogosultságának működtetésére egyaránt érvényesek az Informatikai Biztonsági Szabályzatban rögzített előírások.

VI. Fejezet

ADATVÉDELMET ÉRINTŐ ESEMÉNYEK

23. § (1) Az OAH adatkezelést végző foglalkoztatottja az adatkezeléssel, adatvédelemmel kapcsolatos problémák, adatvédelmi incidens gyanújának észlelése esetén e-mailben és szükség esetén telefonon soron kívül tájékoztatja a szervezeti egységének vezetőjét és az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő – a bejelentett esemény jellegétől függően - az Informatikai és Biztonsági Főosztály, valamint az eseménnyel érintett személy, vagy szervezeti egység bevonásával kielemzi, hogy a bejelentésben közölt probléma pontosan milyen típusú incidenst jelent. Ha megvalósul az adatvédelmi incidens, meg kell állapítani, hogy az csekély jelentőségűnek tekinthető, vagy az adatvédelmi hatóságnak bejelentésre köteles adatvédelmi incidenst foglal magában.

(2) Az adatvédelmi incidenst – ha az kockázattal jár a természetes személyek jogaira és szabadságára nézve – indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, az adatvédelmi tisztviselő a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) online Incidensbejelentő Rendszerén keresztül bejelenti a NAIH-nak. Amennyiben a bejelentés 72 órán belül nem teljesíthető, a bejelentéshez csatolni kell a késedelem okainak részletes indoklását.

(3) A bejelentésben ismertetni kell:

a) az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;

(4) Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

(5) Az adatvédelmi tisztviselő soron kívül írásban tájékoztatja az OAH elnökét az adatvédelmi incidens bekövetkezéséről – a kisebb súlyú incidensről is - és nyilvántartást vezet róluk, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslásukra tett intézkedéseket. A nyilvántartás lehetővé teszi, hogy a NAIH felügyeleti hatóságként ellenőrizze az e cikk követelményeinek való megfelelést.

24. § (1) Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa – figyelemmel annak jellegére, hatókörére, körülményére és céljaira – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az OAH az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

(2) Az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát ki kell kérni.

(3) Az OAH – az adatvédelmi tisztviselő bevonásával – szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

25. § (1) Ha a 24. § szerinti adatvédelmi hatásvizsgálat azt állapítja meg, hogy az adatkezelés az OAH által tervezett kockázatcsökkentő intézkedések hiányában valószínűsíthetően magas kockázattal járna, a személyes adatok kezelése csak azt követően kezdhető meg, hogy az OAH konzultált a felügyeleti hatósággal.

(2) Az OAH a felügyeleti hatósággal folytatott konzultáció során a felügyeleti hatóságot tájékoztatja:

a) adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről

b) a tervezett adatkezelés céljairól és módjairól;

c) az érintettek fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;

d) az adatvédelmi tisztviselő elérhetőségeiről;

e) a lefolytatott adatvédelmi hatásvizsgálatról; és

f) a felügyeleti hatóság által kért minden egyéb információról.

26. § Az iratkezelési tevékenység során megvalósuló adatkezelésre vonatkozó részletes szabályokat az Iratkezelési Szabályzat tartalmazza. Az iratkezelés során végzett adatkezelésekre a jelen Szabályzat rendelkezéseit az Iratkezelési Szabályzattal összhangban kell alkalmazni.

27. § (1) Az OAH megteszi a megfelelő technikai és szervezési intézkedéseket a foglalkoztatottak számára biztosított e-mail-fiókok, számítástechnikai és mobiltelefon eszközök használatával összefüggésben, valamint ennek ellenőrzése során biztosítja a személyes adatok védelmét, és gondoskodik az érintettek megfelelő tájékoztatásáról.

(2) A GDPR alapján a munkahelyi e-mail-fiók, továbbá a foglalkoztatott rendelkezésére bocsátott laptop, illetve mobiltelefon adattartalma személyes adatnak, a személyes adaton elvégzett bármely művelet pedig adatkezelésnek minősül.

(3) A munkahelyi e-mail-fiók és a számítástechnikai eszközök, mobiltelefon áttekintése, ellenőrzése során az OAH kiemelt figyelmet fordít a személyes adatok védelmére, ezért a fokozatosság elvét betartva az alábbi eljárásrendet követi:

a) Az ellenőrzött személyt az ellenőrzést megelőzően tájékoztatni kell a tervezett ellenőrzésről, ennek indokáról annak érdekében, hogy a nem munkavégzési célú személyes adatait saját eszközre másolhassa, illetve azokat törölhesse, töröltethesse. Az ilyen adatmentést az OAH-nak joga és kötelezettsége felügyelni annak érdekében, hogy az valóban csak a magáncélból kezelt adatokra korlátozódjon.

b) Az ellenőrzést megelőzően az adatvédelmi tisztviselőnek egyedi adatkezelési tájékoztatót kell készítenie, amelyben az adatkezelés, az ellenőrzés célját pontosan meg kell határozni. Az ellenőrzés jogalapja az OAH jogos érdeke, ezért az adatvédelmi tisztviselőnek minden egyes ellenőrzés esetében esetileg kell érdekmérlegelést elvégeznie és az érdekmérlegelési tesztet dokumentálnia.

c) Az OAH az ellenőrzés során a fokozatosság elvét betartva köteles eljárni. Ha az ellenőrzés során az e-mail feladóját és tárgyát vizsgálva megállapítható, hogy magáncélú e-mailről van szó, az e-mail megnyitása tilos.

d) Amennyiben nem állapítható meg az e-mail magán jellege, az e-mailt meg lehet nyitni. Amennyiben ebből megállapítható, hogy magáncélú e-mailről van szó, az e-mail további vizsgálatát mellőzni kell.

e) Az e-mail mellékletét abban az esetben lehet megnyitni, amennyiben a magán e-mail jelleg teljességgel kizárható.

f) Az ellenőrzés csak akkor végezhető, ha az ellenőrzött személy vagy képviselője, meghatalmazottja jelen van, és amennyiben magánjellegű személyes adatot érint az ellenőrzés, jogosult azt jelezni. Az ellenőrzést két tanú jelenlétében kell végezni. Az ellenőrzés során jegyzőkönyvet kell felvenni, amelyet az adatvédelmi tisztviselő készít el.

Az adatkezeléssel kapcsolatos alapfogalmak értelmezése a GDPR, valamint az Infotv. alapján

1. **„érintett”:** bármely információ alapján azonosított, vagy azonosítható természetes személy;
2. „**személyes adat**”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ;
3. „**adatkezelés**”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
4. „**az adatkezelés korlátozása**”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
5 „**profilalkotás**”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
6. „**álnevesítés**”: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;
7. „**nyilvántartási rendszer**”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
8. „**adatkezelő**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
9. „**adatfeldolgozó**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
10. „**címzett**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
11. „**harmadik fél**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

12. „**az érintett hozzájárulása**”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
13. „**adatvédelmi incidens**”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
14. „**genetikai adat**”: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;
15. „**biometrikus adat**”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;
16. „**egészségügyi adat**”: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
17. „**tevékenységi központ**”:
    a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
    b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;
18. „**képviselő**”: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;
19. „**vállalkozás**”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;
20. „**vállalkozáscsoport**”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;
21. „**kötelező erejű vállalati szabályok**”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon

csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

22. „**felügyeleti hatóság**”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;
23. „**érintett felügyeleti hatóság**”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:
    a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
    b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
    c) panaszt nyújtottak be az említett felügyeleti hatósághoz;
24. „**személyes adatok határokon átnyúló adatkezelése**”:
    a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
    b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;
25. „**releváns és megalapozott kifogás**”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;
26. „**az információs társadalommal összefüggő szolgáltatás**”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (19) 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;
27. „**nemzetközi szervezet**”: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre, vagy amely ilyen megállapodás alapján jött létre;
28. „**különleges adat”:** a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális irányultságára vonatkozó személyes adatok;
29. **„kötelező adatkezelés**”: az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges illetőleg az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
30. **„adattovábbítás”**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
31. **„nyilvánosságra hozatal”**: az adat bárki számára történő hozzáférhetővé tétele;
32. **„adattörlés”**: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
33. **„adatmegsemmisítés”**: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

34. **„tiltakozás”**: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri.

2. függelék a 8/2026. (VII.1.) elnöki utasításhoz

ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA (GDPR 30. cikk)

Adatkezelés megnevezése	
Adatkezelő neve (illetékes szervezeti egység)	
Adatkezelő elérhetősége	
Az adatkezelés célja vagy céljai	
Az érintettek kategóriái	
Ki férhet hozzá a kezelt személyes adatokhoz?	
A személyes adatok kategóriái (pl. név, lakcím, e-mail cím, fotó stb.)	
A személyes adatok kezelésének jogalapja (jogszabályhely címe, jogszabályhely megadása)	
Mely belső szabályozó dokumentum rendelkezik a személyes adatok kezeléséről?	
Azok a címzettek, akikkel a személyes adatokat közlik vagy közölni fogják (pl. ügyfelek, engedélyesek, állami intézmények, állami hatóságok stb. – magáncégek esetében nem szükséges a cégnevek felsorolása, harmadik országbeli címzettek vagy nemzetközi szervezetek is)	
Adattovábbításra vonatkozó információk (harmadik ország vagy nemzetközi szervezet azonosítása – pl. konferencián részvétel, szakmai látogatás, átadott személyes adatok kategóriái stb.)	
Adatkategóriák törlésére előirányzott határidők (mennyi ideig őrizhetők meg a személyes adatok)	
Az adatkezelés biztonsága érdekében tett technikai és szervezési intézkedések	
Adattárolás formája (papíron vagy elektronikusan)	