FEAK
Független Energetikai Adatközpont Zrt.

Általános adatvédelmi és adatbiztonsági szabályzat

Hatályba lépés dátuma: 2025.július 1.

Verziószám: 0.1

Tartalom

I. ÁLTALÁNOS RENDELKEZÉSEK

1. § (1) Az általános adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a FEAK Független Energetikai Adatközpont Zrt-nél (a továbbiakban: „FEAK") folytatott valamennyi személyes adatok kezelésének jogszerű közös rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

(2) A Szabályzatot az általános adatvédelmi rendelet (a továbbiakban: „általános adatvédelmi rendelet", vagy „GDPR"), valamint a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kibertv.) rendelkezéseire figyelemmel, továbbá az alkalmazandó ágazati jogszabályi követelményekkel összhangban kell alkalmazni.

(3) A FEAK-hoz beérkező és a FEAK-nál keletkezett nyílt iratok készítésének, kezelésének, nyilvántartásának, irattározásának és selejtezésének alapvetői szabályait, az iratkezeléssel összefüggő adatvédelmi és adatbiztonsági szabályokat a FEAK iratkezelésének szabályairól szóló, később kialakítandó ás a Szabályzat függelékeként feltöltendő eljárásrend vagy ezzel egyenértékű vezérigazgatói utasítással összhangban kell alkalmazni.

(4) A FEAK ENAP-HMKE Inverter adatgyűjtő rendszere (a továbbiakban: HMKE EIR) által tárolt és kezelt személyes adatok védelmére irányuló követelményeket a jelen Szabályzat HMKE EIR Adatvédelmi és adatbiztonsági szabályzat című függelékében meghatározottakkal együtt kell alkalmazni.

(5) A Szabályzatot a minősített adatok tekintetében az Adatközpont Szabályzat és mellékletei rendelkezéseivel összhangban kell alkalmazni.

(6) A Szabályzatban meghatározott adatbiztonsági követelményeket az Adatközpont Szabályzat belépésre jogosító biztonsági okmányok és biztonsági kulcsok szabályairól szóló rendelkezéseivel összhangban kell alkalmazni.

(7) A Szabályzat alkalmazása során irányadó fogalmak, rövidítések és definíciók az alábbiak:

- **Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel. [Általános Adatvédelmi Rendelet 4. cikk 8.]
- **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. [Általános Adatvédelmi Rendelet 4. cikk 2.]
- **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. [Általános Adatvédelmi Rendelet 4. cikk 7.] Jelen Adatvédelmi és Adatbiztonsági Szabályzat alkalmazása szempontjából az Energetikai Adatszolgáltató Platform engedélyes.
- **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. [Általános Adatvédelmi Rendelet 4. cikk 8.]

- **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. [Általános Adatvédelmi Rendelet 4. cikk 5.]
- **Adatkezelési Tájékoztató:** a személyes adatok kezelésekre vonatkozó, az Adatvédelmi és Adatbiztonsági Szabályzat mellékletét képező, az Energetikai Adatszolgáltató Platform engedélyes honlapján elérhető tájékoztatók.
- **Általános Adatvédelmi Rendelet (GDPR):** 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 (általános adatvédelmi rendelet) szóló, 2016. április 27-i, 2016/679 európai parlamenti és tanácsi rendelet.
- **DIMOP Projekt:** DIMOP_Plusz-2.1.2-23-2023-00001 Nagytömegű energetikai fogyasztói adatok feldolgozására és azok optimalizálására, ez alapján beavatkozásra alkalmas MI-vel megtámogatott informatikai döntéstámogató rendszerek fejlesztése projekt, amelynek keretében az ENAP rendszer fejlesztése megvalósul.
- **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. [Általános Adatvédelmi Rendelet 4. cikk 11.]
- **ENAP-HMKE Inverter adatgyűjtő rendszere (HMKE EIR):** az ENAP azon funkcióinak összessége, melyek háztartási méretű kiserőmű nem elszámolási célú termelési és üzemeltetési adatait kezelik.
- **HMKE EIR:** ENAP-HMKE Inverter adatgyűjtő rendszere
- **HMKE:** háztartási méretű kiserőmű
- **NAIH**: Nemzeti Adatvédelmi és Információszabadság Hatóság.
- **Személyes adat**: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. [Általános Adatvédelmi Rendelet 4. cikk 1.]

(8) A Szabályzatban alkalmazott további fogalmak tekintetében egyebekben az általános adatvédelmi rendelet 4. cikke szerinti meghatározások az irányadók.

2. § (1) A Szabályzat hatálya kiterjed a FEAK-nál foglalkoztatott valamennyi köztisztviselőre, munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottra (a továbbiakban együtt: foglalkoztatott), továbbá azon személyekre, akik szakmai gyakorlat keretében, vagy kutatási célból a FEAK-nál személyes adatokat ismernek meg.

II. A FEAK ADATVÉDELMI RENDSZERE

A személyes adatok kezelésével kapcsolatos felelősségek a FEAK-nál

3. § (1) A személyes adatok védelméért, az adatkezelés jogszerűségéért a FEAK vezérigazgatója felel. Ennek keretében

a) szabályzatok és kötelező utasítások útján meghatározza a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket és rendelkezik azok folyamatos alkalmazásáról és naprakészen tartásáról;

b) gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági intézményrendszer működtetéséről, a működéshez szükséges intézkedések megtételéről;

c) írásban kijelöli a FEAK adatvédelmi tisztviselőjét;

d) meghozza a FEAK, mint adatkezelő tekintetében az adatkezelésre vonatkozó döntéseket;

e) felel a FEAK adatkezelési tevékenységével kapcsolatos közzétételi kötelezettség teljesítéséért.

(2) A FEAK vezérigazgatója az adatkezelés személyi és tárgyi feltételeinek biztosításáról, a szabályzatban foglaltak végrehajtásáról, az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról az önálló szervezeti egységek vezetői útján, a FEAK Szervezeti és Működési Szabályzatában (a továbbiakban: SZMSZ) meghatározottakkal összhangban gondoskodik.

(3) A FEAK vezérigazgatója az adatkezeléssel kapcsolatos döntések előkészítését, az elszámoltathatóság érdekében szükséges dokumentáció és intézkedések tervezetének összeállítását az adatvédelmi tisztviselő útján végzi.

4. § A FEAK vezérigazgatója maga vagy az adatvédelmi tisztviselő útján gondoskodik a szervezeti egysége állományába tartozó, vagy az amellett foglalkoztatott valamennyi személy kapcsán

a) az adatvédelmi követelmények érvényre juttatásáról;

b) a Szabályzatban vagy más kötelező erejű adatvédelmi előírásban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról;

c) a szükséges hozzáférési jogosultságok kiadására és visszavonására irányuló előterjesztésekről;

d) az adatvédelmi tudatosító – ideértve az adatvédelmi incidenskezeléssel, a kapcsolódó információbiztonsággal, valamint az iratkezeléssel összefüggő ismereteket is – képzéseken történő részvételről, szükség esetén ilyen képzés szervezésének kezdeményezéséről.

5. § (1) A FEAK-nál foglalkoztatottak

a) a Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat;

b) betartják az adatkezelésre vonatkozó jogszabályokban, más belső szabályzatokban foglalt előírásokat;

c) tudásukat naprakészen tartják a munkavégzésükre irányadó adatvédelmi és adatbiztonsági előírások kapcsán és az adatvédelmi incidensek gyanújának felismerése érdekében.

(2) Ha a személyes adatok védelmével kapcsolatos előírások megsértése miatt a FEAK-nak jogerősen sérelemdíj, kártérítés fizetési kötelezettsége keletkezik, a jogsérelmet okozó

foglalkoztatottat, foglalkoztatottakat kártérítési felelősség terheli.

6. § A FEAK adatvédelmi tisztviselője közvetlenül a FEAK vezérigazgatójának felel, függetlenül és befolyásolástól mentesen látja el az általános adatvédelmi rendeletben és az e Szabályzatban meghatározott feladatait.

7. § A FEAK információbiztonsági felelőse segíti a FEAK-ot az adatbiztonsági követelmények teljesítésében. Ennek keretében

a) együttműködik az adatvédelmi tisztviselővel az adatvédelmi intézkedések naprakészen tartásában, valamint a személyes adatok biztonságával kapcsolatos ügyekben,

b) szükség esetén részt vesz az adatvédelmi incidens kivizsgálásában és kezelésében,

c) szükség esetén, felkérésre részt vesz az adatvédelmi hatásvizsgálat lefolytatásában.

A FEAK szervezetén kívüli személyek bevonása az adatkezelés folyamatába

8. § (1) Amennyiben jogszabály, hatóság elírása vagy a FEAK vezérigazgatójának döntése alapján a FEAK feladatának ellátása érdekében adatfeldolgozó igénybevétele szükséges, úgy az általános adatvédelmi rendelet 28. cikke szerinti tartalommal az adatfeldolgozó felelősségét önálló szerződésben vagy a felek között létrejövő szolgáltatási szerződés részeként kell rögzíteni. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

(2) A (1) bekezdésben foglalt kötelezettség nem alkalmazandó annyiban, amennyiben az adatfeldolgozó igénybevételének kereteit és garanciális feltételeit jogszabály határozza meg.

9. § (1) Amennyiben jogszabály, hatóság elírása vagy a FEAK vezérigazgatójának döntése alapján a FEAK feladatának ellátása érdekében közös adatkezelői jogviszony létesítése szükséges, úgy a felek között létrejövő írásbeli megállapodás tartalmazza legalább a GDPR 26. cikke szerinti tartalmi elemeket. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

(2) Az (1) bekezdés alapján létrejött közös adatkezelői megállapodás lényegét a kapcsolódó adatkezelési tájékoztató részeként szükséges az érintett rendelkezésére bocsátani.

10. § A FEAK-kal szerződéses jogviszonyba kerülő önálló adatkezelő mint címzett kapcsán a szerződés részeként szükséges rendelkezni a személyes adatok védelme és biztonsága érdekében alkalmazandó intézkedésekről. A szerződés adatkezelést érintő részének összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

Az adatvédelmi tisztviselő kinevezése, jogállása és feladatai

11. § (1) A FEAK vezérigazgatója határozatlan időre, írásban jelöli ki az adatvédelmi tisztviselőt a FEAK-nál.

(2) Adatvédelmi tisztviselői feladatot nem láthat el olyan személy, aki a FEAK-nál adatkezeléssel kapcsolatos érdemi döntések meghozatalára jogosult személynek a Polgári Törvénykönyvről szóló 2013. évi V. törvény 8:1. § (1) bekezdés 2. pontja szerinti hozzátartozója.

(3) Az adatvédelmi tisztviselő számára biztosítani kell, hogy – a GDPR-ban és más jogszabályban, valamint az e szabályzatban meghatározott feladatainak ellátása céljából és az ahhoz szükséges mértékben – minősített adatot is megismerjen, minősítéssel jelölt iratokba betekinthessen. Az elvárt személyi biztonsági feltételeknek történő megfelelés dokumentált módon történő kialakításáig és igazolásáig nem nevezhető ki az adatvédelmi tisztviselő.

(4) Az adatvédelmi tisztviselő nevét és elérhetőségét a FEAK honlapján közzétett adatkezelési tájékoztatók útján nyilvánosan elérhetővé kell tenni, kijelöléséről a FEAK foglalkoztatottjait írásban tájékoztatni kell.

(5) Az adatvédelmi tisztviselő halaszthatatlan feladatait, így különösen az adatvédelmi incidensek kezelésével kapcsolatos teendőit távollétében, akadályoztatása, vagy érintettsége esetén helyettesítése a FEAK belső szabályzataiban és egyéb dokumentumaiban meghatározottak szerint történik helyettes. A helyettes a feladat ellátását megelőzően esetileg mérlegelni köteles, hogy esetében a Szabályzatban foglalt összeférhetetlenséggel kapcsolatos feltételek megvalósultak-e.

(6) Amennyiben az adatvédelmi tisztviselő az ellátandó feladata kapcsán – összeférhetetlensége, a minősített adatok kezeléséhez szükséges személyi feltételek hiánya, vagy más ok miatt – nem jogosult eljárni, úgy arról haladéktalanul tájékoztatja a FEAK vezérigazgatóját, aki az ügyben a feltételeknek megfelelő eseti helyettest jelöl ki.

12. § (1) A FEAK vezérigazgatója biztosítja az adatvédelmi tisztviselő számára a hozzáférést és a megfelelő jogosultságokat a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adatokhoz, valamint a rendelkezésére bocsátja a feladatai ellátásához és szakmai ismeretei naprakészen tartásához szükséges eszközöket és erőforrásokat.

(2) A FEAK valamennyi arra kijelölt munkavállalója segíti az adatvédelmi tisztviselőt a Szabályzat szerinti feladataik ellátása kapcsán.

(3) A FEAK adatvédelmi tisztviselője feladatait más, a munkaköri leírásában meghatározott kötelezettségei mellett, attól függetlenül köteles ellátni, az adatvédelmi tisztviselői tisztségével összefüggő kötelezettségei és feladatai ellátása során nem utasítható, és e tisztségének ellátásával kapcsolatban közvetlenül a FEAK vezérigazgatójának felel.

(4) Amennyiben az adatvédelmi tisztviselő összeférhetetlenséget állapít meg valamely általa ellátandó feladattal összefüggésben, úgy erről köteles haladéktalanul értesíteni a FEAK vezérigazgatóját, és e feladata kapcsán a jogszerű adatkezelés feltételeinek ellenőrzését a FEAK vezérigazgatója által kijelölt helyettesének delegálni.

13. § (1) Az adatvédelmi tisztviselő a GDPR 39. cikkében foglalt feladatai mellett

a) vezeti a FEAK adatvédelmi nyilvántartását;

b) adatvédelmi ellenőrzési tervet készít, amelyet a FEAK vezérigazgatója hagy jóvá;

c) az adatvédelmi ellenőrzési terv alapján – szükség szerint azon túl is, különösen érintettől érkező, a FEAK adatkezelését érintő panasz, vagy adatvédelmi incidens bekövetkezte esetén – ellenőrzi a FEAK-nál az adatvédelmi és adatbiztonsági követelmények teljesítésülését;

d) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a FEAK részére;

e) a személyes adatok kezelését igénylő új tevékenység ellátásáért felelős szervezeti egység kérésére előzetesen is véleményezi a tervezett adatkezelést;

f) megvizsgálja a FEAK által tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén adatvédelmi hatásvizsgálatot kezdeményez és közreműködik annak lefolytatásában;

g) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodást;

h) új adatkezeléssel járó tevékenység tervezése vagy valamely adatkezelés körülményeinek változása esetén megvizsgálja, hogy szükséges-e azzal kapcsolatban adatkezelési tájékoztató, új adatvédelmi nyilvántartás bejegyzés, vagy más dokumentáció összeállítása, illetőleg a már létező dokumentum módosítása;

i) kezdeményezi a FEAK munkatársainak adatvédelmi tudatosító képzését, részt vesz az ilyen képzéssel kapcsolatos feladatok ellátásában, kijelölés esetén képzést tart;

j) kapcsolatot tart a NAIH-hal és szükség szerint más hatósággal a FEAK-ot érintő adatvédelmi ügyekben,

k) elősegíti az érintetteket megillető jogok gyakorlását, valamint véleményezi a FEAK-hoz érkező, érintetti joggyakorlásra irányuló beadványokra összeállított válaszok tervezetét;

l) részt vesz az adatvédelmi folyamatok folyamatos frissítésében.

14. § (1) A Szabályzat hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó bármely kérdésben – a FEAK belső szabályzatai és szervezeti struktúrájában meghatározott rend betartása nélkül, közvetlenül és szabadon megválasztott kapcsolattartási mód szerint – az adatvédelmi tisztviselőhöz fordulhat.

(2) Saját helyzetéből fakadó okokra hivatkozva bármely érintett jogosult kérni, hogy az adatvédelmi tisztviselő ne fedje fel kilétét a FEAK vezérigazgatója vagy bármely más foglalkoztatottja előtt. Az adatvédelmi tisztviselő a kérésnek köteles eleget tenni, még akkor is, ha ennek hiányában a panaszolt adatvédelmi probléma nem orvosolható, azonban erről köteles tájékoztatni az érintettet.

(3) Az (1) bekezdés szerinti panaszt, ha az annak kivizsgálásához szükséges minden releváns információ rendelkezésre áll, az adatvédelmi tisztviselő köteles 15 napon belül kivizsgálni, és a vizsgálat eredményéről értesíteni az érintettet.

15. § (1) Az adatvédelmi tisztviselő jogosult

a) tájékoztatást, felvilágosítást kérni minden, e Szabályzat hatálya alá tartozó adatkezelésről;

b) minden, e Szabályzat hatálya alá tartozó adatkezelést vizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik;

c) tanácskozási és véleményezési joggal részt venni minden olyan fórumon, ahol a feladatai ellátásával összefüggő kérdések szerepelnek a napirenden,

d) javaslatot tenni közvetlenül a FEAK vezérigazgatójának valamely személyes adatok kezelését érintő kérdésben.

(2) Az adatvédelmi tisztviselő az ellenőrzései kapcsán és a 13. § szerinti vizsgálatával összefüggésben a fentiek mellett

a) felszólíthatja az adatkezelésben résztvevő személyt a jogszerű állapot helyreállítására;

b) kisebb súlyú ügyben közvetlenül az adatkezelésért felelős önálló szervezeti egység vezetőjénél kezdeményezheti az alkalmazott adatkezelési gyakorlat felülvizsgálatát;

c) kezdeményezheti a FEAK vezérigazgatóénél a vonatkozó adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.

III. A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK ÉRVÉNYESÜLÉSE A FEAK-NÁL

Adatkezelés kialakításával összefüggő kötelezettségek

16. § (1) A személyes adatok kezelésével járó új tevékenység megkezdése, vagy a folyamatban lévő adatkezelési tevékenységekkel kapcsolatos módosítások hatályba lépése előtt az SZMSZ alapján a feladat ellátásáért felelős szervezeti egység vezetője kezdeményezi az adatvédelmi tisztviselőnél az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében szükséges és arányos intézkedések meghozatalát.

(2) Az (1) bekezdés szerinti esetben rögzíteni és megfelelően dokumentálni kell a tervezett adatkezelés legfontosabb jellemzőit, így legalább

a) az adatok kezelésére okot adó körülményt, vagy jogszabályi rendelkezést;
b) a feladat ellátásához szükséges adatköröket és azok tervezett forrását;
c) a tervezett vagy jogszabályban meghatározott megőrzési időt, vagy az annak meghatározásához szükséges szempontokat;
d) az ahhoz kapcsolódó adattovábbítás címzettjeit;
e) az adatok biztonsága, valamint az érintettekre nézve azonosított kockázatok csökkentése érdekében tervezett intézkedéseket.

(3) A (2) bekezdés szerintiek alapján az adatvédelmi tisztviselő köteles érdemi vizsgálatra; majd javaslatot tenni a FEAK vezérigazgatójának

a) az ahhoz kapcsolódóan szükségesnek tartott további szervezési és technikai intézkedésekre, vagy a GDPR 5. cikkében foglalt alapelveknek megfelelő adatkezelés kialakításának szempontjaira nézve;
b) a kapcsolódó adatvédelmi hatásvizsgálat szükségessége kapcsán;
c) az ahhoz kapcsolódó adatkezelési tájékoztató tartalmára és esetleges közzétételére vonatkozóan.

(4) Ha a tervezett adatkezelés kapcsán alkalmazandó a hatályos jogszabályok szerinti rendszeres felülvizsgálati kötelezettség – mivel a FEAK közfeladatát megállapító uniós jog, törvény, vagy helyi önkormányzat rendelete az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát nem tartalmazza – a (3) bekezdés szerinti javaslat a rendszeres felülvizsgálat lefolytatásának időpontjára és módjára is ki kell, hogy térjen.

(5) A (3) bekezdés szerinti javaslat kapcsán a FEAK vezérigazgatója által hozott döntésről az adatvédelmi tisztviselő tájékoztatja a személyes adatkezeléssel járó feladat ellátásáért felelős önálló szervezeti egység vezetőjét is, amennyibe van ilyen.

17. § (1) Kizárólag akkor hivatkozható a FEAK adatkezelési tevékenysége kapcsán a GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap helyett más, a GDPR 6. cikkében foglalt jogalap, ha az adatkezelési tevékenység nem szükséges a FEAK közfeladatának ellátásához, vagy közhatalmi tevékenységének gyakorlásához.

(2) Az (1) bekezdésben foglaltakon túl is kizárólag akkor képezheti a FEAK adatkezelésének jogalapját a GDPR 6. cikk (1) bekezdés a) pontja szerinti érintetti hozzájárulás, ha az adatkezelés vonatkozásában igazolható módon nincs az érintett és a FEAK között egyértelműen egyenlőtlen viszony, továbbá szervezési és technikai intézkedésekkel biztosítható, hogy az érintett hozzájárulását bármikor ugyanolyan könnyen visszavonhassa, ahogy azt megadta.

18. § (1) Személyes adatokat továbbítani kizárólag pontosan meghatározott és jogszerű célból, a konkrét esetben közvetlenül hivatkozható jogalap birtokában lehetséges, és a továbbítandó adatok körét az alkalmazandó jogszabályi követelményeket és az iratkezelésre vonatkozó belső előírásokat is mérlegelve az adatkezelés céljához szükséges körre kell szűkíteni.

(2) Amennyiben a FEAK által kezelt személyes adatok továbbítására nem az Adatközpont

Szabályzat és mellékletei, különösen az Adatvédelmi és adatbiztonsági szabályzat című melléklete rendelkezéseivel összhangban és a FEAK iratkezelésének szabályairól szóló, a Szabályzat függelékeként feltöltendő későbbi eljárásrend vagy vezérigazgatói utasításban meghatározott iratkezelő rendszerben iktatott módon kerül sor, úgy arról az adattovábbítással járó feladat ellátásáért felelős önálló szervezeti egység elektronikus úton nyilvántartást köteles vezetni.

Adatbiztonsági követelmények

19. § (1) A FEAK a kezelésében lévő személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosítandó, az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész, zárt, teljes körű és folytonos szervezési és technikai védelmi intézkedéseket alkalmaz.

(2) Az alkalmazott védelmi intézkedések naprakészen tartása érdekében az információbiztonsági vezető és adatvédelmi tisztviselő írásban javaslatot tehet azok pontosítására vagy fejlesztésére a FEAK vezérigazgatójának.

(3) A FEAK elektronikus információs rendszereihez és – a tevékenységével összefüggésben ellátott feladatok ellátásához szükséges – más szerv kezelésében lévő elektronikus információs rendszerekhez, valamint nem elektronikus úton vezetett nyilvántartásokhoz történő hozzáférési jogosultságot és annak szintjét az önálló szervezeti egység vezetőjének kezdeményezésére a FEAK vezérigazgatója – vagy döntése alapján a rendszer üzemeltetéséért vagy eléréséért felelős szervezeti egység vezetője – adja meg, kezdeményezi annak megadását a rendszer üzemeltetőjénél, illetve vonja vissza, vagy kezdeményezi annak visszavonását a rendszer üzemeltetőjénél.

(4) A jogosultságok naprakészségét a nem a FEAK által üzemeltetett rendszerekhez kapcsolódóan a hozzáférést kezdeményező önálló szervezeti egység vezetője köteles évente, dokumentált módon ellenőrizni.

(5) A FEAK feladatellátásával összefüggő személyes adatokat is tartalmazó iratot vagy adathordozót a FEAK épületéből kivinni – munkaköri feladat ellátásának kivételével – csak a FEAK vezérigazgatójának engedélyével lehet. A foglalkoztatott ez esetben is köteles gondoskodni az adatbiztonsági követelmények megvalósulásáról.

(6) A FEAK közös használatú helyiségeiben és közös használatú eszközei kapcsán – így különösen nyomtatók, másológépek, irattárolók esetében – a személyes adatok célhoz kötött felhasználását, valamint integritását és bizalmas jellegét garantáló további előírásokat jogosult a foglalkoztatottak számára meghatározni az érintett önálló szervezeti egység vezetője.

(7) A FEAK-nál szakmai gyakorlatot teljesítő, vagy a FEAK-kal foglalkoztatásra irányuló jogviszonyban nem álló kutatási tevékenységet végző személy a FEAK kezelésében lévő irathoz és elektronikus információs rendszerhez kizárólag titoktartási nyilatkozat aláírását, továbbá a kezelt adatok biztonságát garantáló szervezési és műszaki intézkedések kialakítását követően férhetnek hozzá.

20. § (1) A jogos érdekét igazoló harmadik személy hozzáférési és iratbetekintési jogának személyes, vagy képviselője útján történő gyakorlása során, valamint az eljárás során keletkezett iratról való másolat, kivonat készítésekor kiemelt figyelmet kell fordítani a bizalmasság elvének történő megfelelés érdekében a törvény által előírt garanciákra és korlátozó rendelkezésekre, így különösen a zárt adatkezeléssel kapcsolatos feladatokra.

(2) Telefonos ügyfélszolgálati tevékenység ellátása során a FEAK rendszereiből személyes adatot továbbítani tilos, tekintettel arra, hogy a hívó fél minden kétséget kizáró módon történő azonosítása a FEAK-nál nem lehetséges.

Az adatkezelési műveletek átláthatóságára vonatkozó követelmények

21. § (1) A FEAK adatkezelési tevékenységeire vonatkozóan az adatkezelés érintettje számára világos, könnyen értelmezhető és átlátható módon, az adatkezelés céljai mentén a GDPR 13-14. cikke szerinti tartalommal szükséges az adatkezelési tájékoztatókat összeállítani.

(2) Az adatkezelési tájékoztatókban foglaltak tartalmi megfelelőségét, naprakészségét és elérhetőségét az adatvédelmi tisztviselő és az SZMSZ-ben meghatározott feladataihoz kötődően a tevékenység ellátásáért felelős önálló szervezeti egység is köteles figyelemmel kísérni.

(3) A kizárólag a FEAK foglalkoztatottjait érintő adatkezelési célok kapcsán összeállított adatkezelési tájékoztatókat a FEAK székhelyén elérhető zárt informatikai rendszerében kell a foglalkoztatottak számára elérhetővé tenni.

(4) A FEAK-nál foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, elektronikus úton szükséges megküldeni az őket érintő adatkezelési tájékoztatókat.

(5) A (3)-(4) bekezdésben nem szabályozott érintetti kör esetében a FEAK a honlapján, az „Adatkezelési tájékoztatók” cím alatt közzétéve bocsátja az érintettek rendelkezésére a szükséges tájékoztatást.

Az adatkezelési tevékenységek nyilvántartása

22. § (1) A FEAK adatvédelmi tisztviselője elektronikusan, kizárólag a FEAK székhelyén elérhető zárt informatikai rendszerben vezeti a FEAK adatkezelési tevékenységeinek nyilvántartását.

(2) Az adatkezelési tevékenységek nyilvántartása az adatkezelési célok mentén, a GDPR 30. cikke által meghatározott tartalommal összeállított nyilvántartás bejegyzésekből áll, amelynek összhangban kell lennie a kapcsolódó adatkezelési tájékoztatókban foglaltakkal.

(3) A nyilvántartás aktualizálását, szükséges módosítását az adatvédelmi tisztviselő végzi a Szabályzat 7-9. §-ai és 15. § szerinti tájékoztatások alapján.

Az adatvédelmi hatásvizsgálat lefolytatása

23. § (1) Amennyiben egy tervezett adatkezelés kapcsán az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében foglalt feltételei fennállnak – mivel annak jellege, hatóköre, körülményei és céljai, vagy az alkalmazott technológiai megoldások kapcsán az valószínűsíthetően magas kockázattal jár az érintettre nézve, vagy a tervezett adatkezelés a FEAK által a GDPR 35. cikk (4) bekezdése szerint összeállított jegyzékében szerepel – az adatvédelmi tisztviselő írásban kezdeményezi annak lefolytatását a FEAK vezérigazgatójánál.

(2) Az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében foglalt feltételei fennállásának vizsgálata keretében figyelemmel kell lenni arra is, hogy alkalmazható-e valamely, a lefolytatás kötelezettsége alóli kivételszabály, így különösen a kötelező adatkezelést előíró

jogszabály kapcsán készült-e adatvédelmi hatásvizsgálat, illetve elérhető-e azonos tárgyban készült adatvédelmi hatásvizsgálat.

(3) Az (1) bekezdés szerinti feljegyzés tartalmazza

a) az adatvédelmi hatásvizsgálat lefolytatására okot adó legfontosabb szempontokat;

b) a 15. § (2) bekezdés szerinti tartalmat;

c) az alkalmazni javasolt módszertan megjelölését;

d) az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba bevonni tervezett szervezeti egységeket és személyeket, amennyiben nem az adatvédelmi tisztviselő egymaga végzi az adatvédelmi hatásvizsgálatot;

e) a tervezett adatkezelés érintettjei véleményének kikérése kapcsán javasolt megoldást, vagy annak jogszerű mellőzésére okot adó körülményeket;

f) amennyiben az előre megítélhető, a hatásvizsgálat lefolytatásának tervezett időrendjét.

(4) A FEAK vezérigazgatója kikéri az adatvédelmi tisztviselő álláspontját az adatvédelmi hatásvizsgálat szükségessége kapcsán, majd elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait.

24. § (1) Amennyiben nem az adatvédelmi tisztviselő egymaga végzi az adatvédelmi hatásvizsgálatot, úgy az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba a FEAK vezérigazgatója a tervezett adatkezeléssel érintett önálló szervezeti egységekből kijelöli a további tagokat.

(2) Az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott –, az adatvédelmi hatásvizsgálatra vonatkozó hatályos iránymutatásban foglalt szempontokat és eljárásrendet a munkacsoport köteles figyelembe venni.

(3) Az adatvédelmi tisztviselő, illetve amennyiben nem az adatvédelmi tisztviselő egymaga végzi az adatvédelmi hatásvizsgálatot, úgy a munkacsoport az adatvédelmi hatásvizsgálat lefolytatását követően megállapításairól és javaslatairól összefoglaló jelentést készít a FEAK vezérigazgatójának. Az adatvédelmi tisztviselő, illetve a munkacsoport tevékenysége során keletkezett iratanyag a jelentés kivételével döntés-előkészítő iratnak minősül.

(4) Amennyiben nem az adatvédelmi tisztviselő egymaga végzi az adatvédelmi hatásvizsgálatot, úgy az adatvédelmi hatásvizsgálatot lefolytató munkacsoport munkáját az adatvédelmi tisztviselő – és amennyiben az adatkezelés elektronikus információs rendszert is érint, a FEAK információbiztonsági felelőse – segíti. Véleményét legalább a kockázatelemzés, a tervezett intézkedések és az összefoglaló jelentés kapcsán ki kell kérni.

(5) Az adatvédelmi hatásvizsgálatról készült jelentést és a kapcsolódó véleményeket a FEAK vezérigazgatója részére írásban kell előterjeszteni. A tervezett adatkezelés nem kezdhető meg, amíg a FEAK vezérigazgatója el nem fogadja

a) az adatvédelmi hatásvizsgálat eredményes lezárultáról, és az abban a kockázatok csökkentését szolgáló intézkedések bevezetéséről és az adatkezelés jóváhagyásáról szóló jelentést, vagy

b) az adatvédelmi hatásvizsgálat mellőzésének, vagy megszüntetésének okait tartalmazó jelentést.

(6) Amennyiben jogszabály valamely, a FEAK által tervezett adatkezelés kapcsán a GDPR 36. cikke szerinti előzetes konzultációt írna elő, vagy az adatvédelmi hatásvizsgálatot lefolytató

munkacsoport annak szükségessége mellett dönt, a FEAK vezérigazgatója eseti jelleggel jelöli ki az abban a FEAK nevében eljáró személyeket úgy, hogy a munkacsoportban résztvevő személyek és a tervezett adatkezeléssel érintett önálló szervezeti egység foglalkoztatottjai abban nem járhatnak el.

IV. AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉVEL KAPCSOLATOS FELADATOK

25. § (1) Amennyiben a FEAK bármely foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja arról az önálló szervezeti egységének vezetőjét vagy az adatvédelmi tisztviselőt. Az önálló szervezeti egység vezetője az általa észlelt adatvédelmi incidens kapcsán saját hatáskörben jár el.

(2) Az önálló szervezeti egység vezetője vagy az általa kijelölt személy az (1) bekezdés szerinti jelzést követően azonnal tájékozódik az eset lényeges körülményeiről.

(3) Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az azt észlelő önálló szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be az adatvédelmi incidens, soron kívül megkezdi az incidens érintettekre nézve megjelenő hatásainak csökkentését és arról haladéktalanul írásban értesíti az adatvédelmi tisztviselőt.

(4) A (3) bekezdés szerinti értesítés az adatvédelmi incidens bekövetkeztének, illetőleg az általa az érintettre nézve jelentett kockázatok és annak hatásainak megállapítása érdekében tartalmazza legalább

a) az adatvédelmi incidens jellegét és rövid leírását, ideértve különösen az észlelés és bekövetkezés feltételezett időpontját, az érintett rendszer vagy irat megjelölését;

b) a valószínűsíthetően érintett személyek körét;

c) a valószínűsíthetően érintett személyes adatok kategóriáit, nagyságrendjét;

d) az általa megtett halaszthatatlan intézkedéseket;

e) megítélése szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyosságát,

f) az általa tervezett további intézkedések leírását.

(5) Az önálló szervezeti egység vezetője haladéktalanul értesíti az adatvédelmi tisztviselőt a bekövetkezett eseményről és a nála rendelkezésre álló információról, ha

a) az adatvédelmi incidens bekövetkezte vagy annak (4) bekezdés szerinti jellemzői számára nem állapíthatók meg egyértelműen és legfeljebb az észlelését követő 24 órán belül,

b) az adatvédelmi incidens megítélése szerint elsősorban más önálló szervezeti egység tevékenységét érinti, illetőleg

c) az adatvédelmi incidens több önálló szervezeti egységet is érinthet.

(6) Az adatvédelmi tisztviselő megvizsgálja a (4) vagy (5) bekezdés szerinti értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja a FEAK információbiztonsági felelősét, az önálló szervezeti egység vezetőjét vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.

(7) Abban az esetben, ha az adatvédelmi incidens feltételezhetően a FEAK által üzemeltetett elektronikus információs rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő a FEAK információbiztonsági felelőse felé is köteles jelezni a bejelentést. A FEAK információbiztonsági felelőse a jelzést követően köteles haladéktalanul véleményt

összeállítani az adatvédelmi tisztviselőrészére arról, hogy az adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismerteti az ezzel kapcsolatos javasolt, valamint megtett intézkedéseket.

(8) Amennyiben az adatvédelmi incidens a FEAK által igénybevett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások (6) bekezdés szerinti kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni.

(9) Az adatvédelmi tisztviselő a (6) bekezdés szerinti vizsgálata keretében mérlegeli az adatvédelmi incidens következtében az érintettekre nézve megjelenő kockázatokat. Ennek során legalább a következőket veszi figyelembe:

a) az adatvédelmi incidens jellegét;

b) az érintettek körét, hozzávetőleges számukat;

c) az incidenssel érintett adatok kategóriáit, az érintett különleges adatokat és a GDPR preambulumának (75) bekezdése szerinti szenzitív adatokat és azok hozzávetőleges számát, illetve nagyságrendjét;

d) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

e) minden, az adatvédelmi incidens megoldására tett vagy tervezett intézkedést, ideértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;

f) az elektronikus információbiztonságot is érintő incidensek esetén az információbiztonságért felelős szervezeti egység vezetője által azonosított további kockázatot;

g) az adatvédelmi incidensek kezelése és a kapcsolódó kockázatok mérlegelése tárgyában az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott – iránymutatást;

h) az adatkezelés kapcsán korábban lefolytatott adatvédelmi hatásvizsgálat dokumentációját.

26. § (1) Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban tájékoztatja a FEAK vezérigazgatóját az adatvédelmi incidens kapcsán tett megállapításairól és az érintettre nézve megjelenő valószínűsített kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.

(2) A szóban nyújtott tájékoztatást és a kezelésre vonatkozó javaslatokat az adatvédelmi incidens elhárítását követően kell írásba foglalni.

(3) Amennyiben a FEAK vezérigazgatója a kapott tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő a FEAK honlapjáról letölthető formanyomtatvány alkalmazásával és a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a FEAK által vezetett nyilvántartásba.

(4) Amennyiben a Szabályzat 24. § (6) bekezdése szerinti vizsgálatot az adatvédelmi tisztviselő véleménye szerint

a) nem lehet 72 órán belül teljeskörűen lefolytatni, vagy

b) nem lehet megállapítani egyértelműen a rendelkezésre álló adatok alapján az adatvédelmi incidenssel érintettek körét, az azzal érintett adatkört, vagy az adatvédelmi

incidens bekövetkezésének valamennyi más lényeges körülményét,

úgy az adatvédelmi tisztviselő a rendelkezésre álló adatok alapján, szakaszos bejelentésre tesz javaslatot a FEAK vezérigazgatója részére. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.

(5) A (3) vagy (4) bekezdés szerinti bejelentés kapcsán induló FEAK általi ellenőrzés vagy adatvédelmi eljárás lefolytatásában a 24. § (6) bekezdés szerinti vizsgálatba bevont, vagy az adatvédelmi incidenssel érintett személy nem vehet részt.

27. § (1) Amennyiben a FEAK vezérigazgatója a 25. § szerinti tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az esemény egyéb körülményei alapján azt szükségesnek látja, a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével elrendeli az érintettek tájékoztatását az adatvédelmi incidens kapcsán.

(2) Amennyiben az adatvédelmi incidenssel érintett természetes személyek tájékoztatására – különösen az érintettek köre vagy a kapcsolattartási adatok biztonságának sérülése miatt – észszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi a FEAK honlapján.

28. § (1) Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint, személyes adatokat nem tartalmazó, a FEAK székhelyén elérhető zárt elektronikus információs rendszerben vezet nyilvántartást, amely tartalmazza

a) az adatvédelmi incidensről készült feljegyzés iktatószámát;

b) az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját;

c) az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;

d) az érintett személyes adatok körét;

e) az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;

f) a 25. § (3) és (4) bekezdés szerinti bejelentés időpontját – amennyiben az adatvédelmi incidenst a FEAK részére a GDPR 33. cikk (1) bekezdése szerint bejelentették, vagy annak rövid indokolását, ami miatt az adatvédelmi incidenst nem jelentették be.

V. AZ ÉRINTETTI JOGGYAKORLÁS BIZTOSÍTÁSÁRA VONATKOZÓ ELŐÍRÁSOK

29. § (1) A FEAK – a GDPR 5. cikkében foglalt adatkezelési elvek sérelme nélkül, a GDPR 32. cikke szerinti technikai és szervezési intézkedések végrehajtás mellett – a FEAK adatkezelésére vonatkozó, érintetti joggyakorlásra irányuló minden beadvány kapcsán – a GDPR 13-14. cikk szerinti tájékoztatás kivételével – esetileg és érdemben vizsgálja azt, hogy elsősorban a kérelmet benyújtó természetes személy kilétével, másodsorban az adatkezelés érintettje FEAK általi azonosításával kapcsolatban merülhetnek-e fel kétségek.

(2) Az érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy személyazonosságának megállapítása érdekében további intézkedéseket indokolt tenni különösen, ha az

a) a kérelmező személyének azonosítását nem biztosító elektronikus levélben, elektronikus aláírás nélkül vagy
b) nem a polgári perrendtartásról szóló 2016. évi CXXX. törvény 325. §-a által meghatározott teljes bizonyító erejű magánokiratba vagy közokiratba foglalt postai küldeményként

került megküldésre a FEAK részére.

(3) A kérelmet benyújtó természetes személy azonosítása érdekében kizárólag az adott célra szükséges és elégséges többlet személyes adat kérhető. Valamely okiratról készült egyszerű elektronikus másolat, vagy nem hitelesített nem elektronikus másolat megküldése a személy azonosítására nem alkalmas, ezért e célra azok megküldését a kérelmet előterjesztő személytől kétség felmerülése esetén sem lehet kérni.

(4) A FEAK az ellenkező bizonyításáig a kérelmet előterjesztő személy megfelelő azonosításának ismeri el a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket.

(5) Amennyiben egy érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy kilétével kapcsolatban nem merül fel kétség, azonban a FEAK által kezelt adatok körében megállapítást nyer, hogy az érintett nem azonosítható, – így különösen mert a FEAK adatkezelésének célja nem teszi szükségessé az érintettnek a FEAK általi azonosítását és bizonyítani tudja, nincs abban a helyzetben, hogy azonosítsa az érintettet – erről haladéktalanul írásban tájékoztatja a kérelmet benyújtó személyt.

(6) Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik a FEAK-hoz, és az abban foglalt – a GDPR 15. cikke szerinti hozzáférési joggyakorlásra, vagy az adatok másolatának kiadására irányuló – kérés olyan adatokra vonatkozik, amelyek megőrzési ideje a FEAK-nál a kérelemtől számítva rövidebb, mint 1 hónap, akkor a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas kérelemmel érintett adatok kezelését az azonosítást lehetővé tevő kérelem beérkezéséig, de legfeljebb 1 hónapig korlátozza.

(7) Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik a FEAK-hoz, és abban valamely érintett kapcsolattartási adataira vonatkozó helyesbítéshez való jog gyakorlására irányuló kérelem van, a FEAK hivatalból is köteles vizsgálni, hogy az általa kezelt kapcsolattartási adatok naprakészek-e. A pontosság elvének történő megfelelés érdekében különösen a FEAK által kezelt adatok összevetése lehet indokolt a személyiadat- és lakcímnyilvántartásban nyilvántartott és a Rendelkezési Nyilvántartásban szereplő adatokkal.

30. § (1) Az érintetti jogok gyakorlására irányuló kérelem elintézésébe az adatvédelmi tisztviselőt be kell vonni. A FEAK-hoz bármely módon - akár nem hivatalos elérhetőségein keresztül, vagy nem megfelelő módon, esetleg formában - előterjesztett, érintetti joggyakorlásra irányuló kérelmet köteles az azt fogadó önálló szervezeti egység vezetője soron kívül az adatvédelmi tisztviselő részére is továbbítani.

(2) Az érintetti joggyakorlásra utaló beadványok kapcsán – az adatvédelmi tisztviselő bevonásával – mindenekelőtt meg kell állapítani, hogy abban az általános adatvédelmi rendelet szerinti valamely érintetti jogot, különösen a GDPR 15. cikke szerinti hozzáférési jogot, vagy más, az Ákr. 33-34. §-a szerinti iratbetekintési jogát kívánja-e gyakorolni a beadványozó, esetleg közérdekű adatigénylést kíván-e előterjeszteni.

(3) Az érintetti joggyakorlások teljesítése során a kérelem tárgyában érintett önálló szervezeti egységek közreműködésével vizsgálni szükséges a FEAK elektronikus iratkezelő rendszerét, és a FEAK által üzemeltetett elektronikus információs rendszereit is.

(4) A FEAK a hozzáférési jog biztosítása során a harmadik fél jogainak védelmét szem előtt tartva jár el az adatokról készített másolat és az azokba történő betekintés biztosítása során is.

31. § (1) A FEAK indokolatlan késedelem nélkül és a lehető legrövidebb időn belül, de legkésőbb az azonosítható érintettől származó kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

(2) Amennyiben annak a GDPR 12. cikkében foglalt feltételei fennállnak, a válaszadás határideje a FEAK vezérigazgatójának döntése szerint további két hónappal meghosszabbítható, azonban ennek megítélése kapcsán részére az (1) bekezdés szerinti határidőn belül, írásban kell igazolni a késedelem okait, és előterjeszteni a hosszabbítás kapcsán az érintettnek nyújtandó tájékoztatás tervezetét.

(3) A FEAK az érintett részére a kérelmével kapcsolatos tájékoztatást az általa a Rendelkezési Nyilvántartásban történt rendelkezéseit figyelembe véve nyújtja. Ilyen rendelkezés hiányában az érintett kérelmében foglaltaknak megfelelő módon, kivételes esetben és arról jegyzőkönyv egyidejű felvétele mellett személyesen is megadhatja.

(4) Az elektronikus úton biztonságosan nem továbbítható személyes adatokat a FEAK postai úton, tértivevényes küldeményben, elektronikus adathordozón küldi meg az érintett részére, vagy külön kérésére jegyzőkönyv egyidejű felvétele mellett azt személyesen adja át.

VI. FÜGGELÉK

1. HMKE EIR Adatvédelmi és Adatbiztonsági Szabályzat
2. Általános munkavállalói adatkezelési tájékoztató
3. Szerződéses partnerek közreműködői részére irányadó adatvédelmi tájékoztató