Sásdi Közös Önkormányzati Hivatal

A Sásdi Közös Önkormányzati Hivatal adatvédelmi és adatbiztonsági szabályzata

Hatályos 2025. december 1. napjától

Adatvédelmi és adatbiztonsági szabályzat

I. Fejezet

ÁLTALÁNOS RENDELKEZÉSEK

1. § (1) Az adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a Sásdi Közös Önkormányzati Hivatalban (továbbiakban: Hivatal), Sásd Város Önkormányzata, Felsőegerszeg Község Önkormányzata, Gödre Község Önkormányzata, Meződ Község Önkormányzata, Oroszló Község Önkormányzata, Palé Község Önkormányzata, Varga Község Önkormányzata, Vázsnok Község Önkormányzata, továbbá a Sásdi Szociális Társulás és a Nyugat-Hegyháti Önkormányzati Társulás tevékenysége során folytatott adatkezelés működésének jogszerű 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 az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2. § (2) bekezdése szerint azt kiegészítő előírásokra figyelemmel, továbbá az alkalmazandó ágazati jogszabályi követelményekkel összhangban kell alkalmazni.

(3) A Hivatalhoz beérkező és a Hivatalnál keletkezett nyílt iratok készítésének, kezelésének, nyilvántartásának, irattározásának és selejtezésének alapvetői szabályait, az iratkezeléssel összefüggő adatvédelmi és adatbiztonsági szabályokat a Hivatal iratkezelési szabályzatával összhangban kell alkalmazni.

(4) A Hivatal elektronikus információs rendszereiben tárolt személyes adatok védelmére irányuló követelményeket az Informatikai Biztonság Szabályzatában meghatározottakkal összhangban kell alkalmazni.

(5) A Hivatal közszolgálati személyi adatkezelésére, a közszolgálati adatvédelem rendjére, az ügykezelési eljárásra, az iratkezelés rendjére, a közérdekű adatok közzétételére a közérdekű adatok megismerésének és a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjére, a tűzvédelemre, a munkavédelemre, a munkavédelem rendjére, az e tárgykörben kiadott szabályzatok rendelkezései irányadóak azzal, hogy az ott nem részletezett, illetőleg szabályozott kérdésekre e szabályzat rendelkezéseit kell alkalmazni.

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

2. § A Szabályzat hatálya kiterjed a Hivatalnál 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 Hivatalnál személyes adatokat ismernek meg.

II. Fejezet

A HIVATAL ADATVÉDELMI RENDSZERE

A személyes adatok kezelésével kapcsolatos felelősségek

3. § (1) A személyes adatok védelméért, az adatkezelés jogszerűségéért a Hivatal vezetője, a jegyző 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 Hivatal adatvédelmi tisztviselőjét;

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

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

(2) A jegyző 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 Hivatal Szervezeti és Működési Szabályzatában (a továbbiakban: SZMSZ) meghatározottakkal összhangban gondoskodik.

(3) A jegyző az adatkezeléssel kapcsolatos döntések előkészítését, az elszámoltathatóság érdekében szükséges dokumentáció és intézkedések tervezetének összeállítását a Titkárság útján végzi.

4. § Az önálló szervezeti egység vezetője gondoskodik a szervezeti egysége állományába tartozó, vagy az amellett foglalkoztatott személyek 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 Hivatalnál 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 Hivatalnak jogerősen sérelemdíj, kártérítés fizetési kötelezettsége keletkezik, a jogsérelmet okozó foglalkoztatottat, foglalkoztatottakat a Küt. 86. §-a szerinti kártérítési felelősség terheli.

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

A Hivatal szervezetén kívüli személyek bevonása az adatkezelés folyamatába

7. § (1) Amennyiben a Hivatal közfeladatának 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.

8. § (1) Amennyiben a jegyző döntése alapján a Hivatal közfeladatának 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.

9. § A Hivatallal 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

10. § (1) A jegyző határozatlan időre, írásban jelöli ki az adatvédelmi tisztviselőt a Hivatalnál adatvédelmi területen szerzett legalább 1 éves tapasztalattal és adatbiztonsági ismeretekkel, valamint szakmai rátermettséggel egyaránt rendelkező köztisztviselők közül.

(2) Adatvédelmi tisztviselői feladatot nem láthat el olyan személy, aki a Hivatalnál adatkezeléssel kapcsolatos érdemi döntések meghozatalára jogosult személy 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 a köztisztviselő nem nevezhető ki adatvédelmi tisztviselőnek.

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

11. § (1) A jegyző 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 Titkárság segíti az adatvédelmi tisztviselőt a Szabályzat szerinti feladata ellátása kapcsán, valamint felel a Hivatal online adatvédelmi tisztviselő bejelentő rendszerében és az adatkezelési tájékoztatókban az adatvédelmi tisztviselő nevének és elérhetőségének naprakészen tartásáért.

(3) A Hivatal 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 jegyzőnek felel.

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

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

a) vezeti a Hivatal adatvédelmi nyilvántartását;

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

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

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

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

f) megvizsgálja a Hivatal 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 Hivatal munkatársainak adatvédelmi tudatosító képzését, részt vesz az ilyen képzéssel kapcsolatos feladatok ellátásában, kijelölés esetén képzést tart;

j) elősegíti az érintetteket megillető jogok gyakorlását, valamint véleményezi a Hivatalhoz érkező, érintetti joggyakorlásra irányuló beadványokra összeállított válaszok tervezetét.

13. § (1) A Szabályzat hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó bármely kérdésben – a hivatali út 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 Hivatal vezetője 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.

14. § (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 Hivatal vezetőjének 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 jegyzőnél a vonatkozó adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.

III. Fejezet

A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK ÉRVÉNYESÜLÉSE A HIVATALNÁL

Adatkezelés kialakításával összefüggő kötelezettségek

15. § (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 a Titkárságnál az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében szükséges és arányos intézkedések meghozatalát.

(2) Az (1) bekezdés szerinti megkeresésben az adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetője rögzíti 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 szerinti értesítést a Titkárság köteles érdemben megvizsgálni; az adatvédelmi tisztviselő véleményét azzal kapcsolatban kikérni; majd az alapján – szükség esetén az előterjesztő szervezeti egységgel történő konzultáció, az értesítés kiegészítése vagy pontosítására történő felhívást követően – javaslatot tenni a jegyzőnek

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 az Infotv. 5. § (5) bekezdésében meghatározott rendszeres felülvizsgálati kötelezettség – mivel a Hivatal 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 jegyző által hozott döntésről a Titkárság tájékoztatja a személyes adatkezeléssel járó feladat ellátásáért felelős önálló szervezeti egység

vezetőjét, valamint a tevékenység adatvédelmi nyilvántartásba történő bejegyzése érdekében az adatvédelmi tisztviselőt.

16. § (1) Kizárólag akkor hivatkozható a Hivatal 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 az Adatkezelő közfeladatának ellátásához, vagy közhatalmi tevékenységének gyakorlásához.

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

17. § (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 Hivatal által kezelt személyes adatok továbbítására nem a Hivatal iratkezelési szabályzatában 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

18. § (1) A Hivatal 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 SZMSZ szerinti feladatkörük kapcsán az önálló szervezeti egységek vezetői, valamint az adatvédelmi tisztviselő írásban javaslatot tehet azok pontosítására vagy fejlesztésére a jegyzőnek.

(3) A Hivatal 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 Jegyző – 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 Hivatal által üzemeltetett rendszerekhez kapcsolódóan a hozzáférést kezdeményező önálló szervezeti egység vezetője köteles évente, dokumentált módon ellenőrizni.

(5) A Hivatal feladatellátásával összefüggő személyes adatokat is tartalmazó iratot vagy adathordozót a Hivatal épületéből kivinni – munkaköri feladat ellátásának kivételével – csak a

jegyző engedélyével lehet. A foglalkoztatott ez esetben is köteles gondoskodni az adatbiztonsági követelmények megvalósulásáról.

(6) A Hivatal 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 Hivatalnál szakmai gyakorlatot teljesítő személy a Hivatal kezelésében lévő irathoz és elektronikus információs rendszerhez kizárólag titoktartási nyilatkozat aláírását, továbbá a kezelt adatok biztonságát garantáló szervezési és műszaki intézkedések kialakítását követően férhet hozzá.

19. § (1) Az ügyfél és jogos érdekét igazoló harmadik személy az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) hatálya alá tartozó eljárásban 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 Hivatal rendszereiből személyes adatot továbbítani tilos, tekintettel arra, hogy a hívó fél minden kétséget kizáró módon történő azonosítása nem lehetséges.

Az adatkezelési műveletek átláthatóságára vonatkozó követelmények

20. § (1) A Hivatal 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 Hivatalnál foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, elektronikus úton szükséges megküldeni az őket érintő adatkezelési tájékoztatókat.

(5) A Hivatal székhelyén vagy telephelyén (kirendeltség) személyesen megjelenő érintetteket, a rájuk vonatkozó adatkezelésekről a Hivatal portaszolgálatánál, a kirendeltségen pedig a bejáratnál elérhető papíralapú adatkezelési tájékoztató útján kell tájékoztatni. Emellett szükség esetén, így különösen látássérültek vagy olvasási, szövegértési képességükben korlátozott érintettek esetében szóbeli tájékoztatás nyújtása is kötelező.

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

Az adatkezelési tevékenységek nyilvántartása

21. § (1) A Hivatal adatvédelmi tisztviselője elektronikusan vezeti a Hivatal 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

22. § (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 Hivatal által a GDPR 35. cikk (4) bekezdése szerint összeállított jegyzékében szerepel – a jegyző rendeli el annak lefolytatását.

(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 tervezett adatkezelést kezdeményező önálló szervezeti egység 15. § (2) bekezdés szerinti tartalommal összeállított megkeresését;

c) az alkalmazni javasolt módszertan megjelölését;

d) az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba bevonni tervezett szervezeti egységeket és személyeket;

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 jegyző kikéri az adatvédelmi tisztviselő álláspontját az adatvédelmi hatásvizsgálat szükségessége kapcsán, majd elrendeli az adatvédelmi hatásvizsgálat lefolytatását.

23. § (1) Az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba a tervezett adatkezeléssel érintett önálló szervezeti egységek kötelesek résztvevőt kijelölni.

(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) A munkacsoport az adatvédelmi hatásvizsgálat lefolytatását követően megállapításairól és javaslatairól összefoglaló jelentést készít a jegyzőnek. A munkacsoport tevékenysége során keletkezett iratanyag a jelentés kivételével döntés-előkészítő iratnak minősül.

(4) Az adatvédelmi hatásvizsgálatot lefolytató munkacsoport munkáját az adatvédelmi tisztviselő – és amennyiben az adatkezelés elektronikus információs rendszert is érint, az elektronikus információs rendszer biztonságáért felelős személy – 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 jegyző részére írásban kell előterjeszteni. A tervezett adatkezelés nem kezdhető meg, amíg a

jegyző 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 Hivatal által tervezett adatkezelés kapcsán a GDPR 36. cikke szerinti előzetes konzultációt írna elő, vagy az adatvédelmi hatásvizsgálatot lefolytató munkacsoport annak szükségessége mellett dönt, a jegyző eseti jelleggel jelöli ki az abban a Hivatal nevében eljáró személyeket úgy, hogy a munkacsoportban résztvevő személyek és a tervezett adatkezeléssel érintett önálló szervezeti egység foglalkoztatottjai abban nem járhatnak el.

IV. Fejezet

AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉVEL KAPCSOLATOS FELADATOK

24. § (1) Amennyiben a Hivatal foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja arról az önálló szervezeti egységének vezetőjét. 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 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 Hivatal által üzemeltetett elektronikus információs rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő a Hivatal elektronikus információbiztonságért felelős vezetője felé is köteles jelezni a bejelentést. A Hivatal elektronikus információbiztonságért felelős vezetője a jelzést követően köteles haladéktalanul véleményt összeállítani az adatvédelmi tisztviselő részére 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 Hivatal 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 elektronikus 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.

25. § (1) Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban tájékoztatja a jegyzőt 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 jegyző 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 GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a Hivatal 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 jegyző 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 Hivatali ellenőrzés vagy adatvédelmi hatósági eljárás lefolytatásában a 24. § (6) bekezdés szerinti vizsgálatba bevont, vagy az adatvédelmi incidenssel érintett személy nem vehet részt.

26. § (1) Amennyiben a Jegyzőa 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 Hivatal honlapján.

27. § (1) Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk

(5) bekezdése szerint, személyes adatokat nem tartalmazó elektronikus nyilvántartás, 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 hatóság részére a GDPR 33. cikk (1) bekezdése szerint bejelentették, vagy annak rövid indokolását, ami miatt az adatvédelmi incidenst nem jelentették be.

V. Fejezet

AZ ÉRINTETTI JOGGYAKORLÁS BIZTOSÍTÁSÁRA VONATKOZÓ ELŐÍRÁSOK

28. § (1) A Hivatal – a GDPR 5. cikkében foglalt adatkezelési elvek sérelme nélkül, a GDPR 32. cikke szerinti technikai és szervezési intézkedések végrehajtás mellett – a Hivatal 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 Hivatal 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,

b) telefax útján, vagy

c) 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 Hivatal 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 Hivatal az ellenkező bizonyításáig a kérelmet előterjesztő személy megfelelő azonosításának ismeri el az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 18. §-a szerint megvalósuló beadványokat, a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket és a Hivatal ügyfélszolgálatán a személyazonosság okirattal történő előzetes igazolását követően személyesen előterjesztett beadványokat.

(5) Amennyiben egy érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy kilétével kapcsolatban nem merül fel kétség, azonban a Hivatal által kezelt adatok körében megállapítást nyer, hogy az érintett nem azonosítható, – így különösen mert a Hivatal adatkezelésének célja nem teszi szükségessé az érintettnek a Hivatal 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 Hivatalhoz, 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 Hivatalnál 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 Hivatalhoz, és abban valamely érintett kapcsolattartási adataira vonatkozó helyesbítéshez való jog gyakorlására irányuló kérelem van, a Hivatal hivatalból is köteles vizsgálni, hogy az általa kezelt kapcsolattartási adatok naprakészek-e. A pontosság elvének történő megfelelés érdekében különösen a Hivatal által kezelt adatok összevetése lehet indokolt a személyiadat- és lakcímnyilvántartásban nyilvántartott és a Rendelkezési Nyilvántartásban szereplő adatokkal.

29. § (1) Az érintetti jogok gyakorlására irányuló kérelem elintézésébe az adatvédelmi tisztviselőt be kell vonni. A Hivatalhoz 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 Hivatal elektronikus iratkezelő rendszerét, és a Hivatal által üzemeltetett elektronikus információs rendszereit is.

(4) A Hivatal 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.

30. § (1) A Hivatal 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 jegyző 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 Hivatal 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 Hivatal postai úton küldi meg az érintett részére, vagy külön kérésére jegyzőkönyv egyidejű felvétele mellett azt személyesen adja át.

Záró rendelkezések

Ez a szabályzat 2025. december 1. napján lép hatályba, egyidejűleg hatályát veszti a tárgyban kiadott, 2020. május 10. napjától hatályos szabályzat.

E szabályzat rendelkezéseit a folyamatban lévő ügyekre is alkalmazni kell.

Sásd, 2025. november 27.

Koszorus Tímea
jegyző