KIFÜ

A Kormányzati Informatikai Fejlesztési Ügynökség elnökének

8/2019. számú utasítása

a KIFÜ adatvédelmi és adatbiztonsági szabályzatáról

I. ÁLTALÁNOS RENDELKEZÉSEK

1 BEVEZETÉS

1.1 A Kormányzati Informatikai Fejlesztési Ügynökség (a továbbiakban: KIFÜ) hatályos Szervezeti és Működési Szabályzatának (a továbbiakban: SzMSz) 14. i) pontja alapján az elnök a KIFÜ vezetése során, amennyiben az irányító szerv vagy jogszabály nem írja elő az irányító szerv egyetértését – figyelemmel az államháztartásról szóló törvény végrehajtásáról rendelkező 368/2011. (XII. 31.) Korm. rendelet (a továbbiakban: Ávr.) 13. § (2) bekezdésében előírtakra is – kiadja a KIFÜ egyéb belső szabályzatait.

1.2 Az utasítás célja

1.2.1 A KIFÜ jelen utasítás (a továbbiakban: utasítás) megalkotásával és hozzáférhetővé tételével biztosítani kívánja az érintettek részére az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR) 12. cikkében meghatározott tájékoztatáshoz való jog érvényesülését. Az utasítás célja, hogy biztosítsa a személyes adatokat tartalmazó nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, valamint meg kívánja akadályozni a személyes adatokhoz való jogosulatlan hozzáférést, azok jogosulatlan megváltoztatását vagy nyilvánosságra hozatalát.

1.3 Az utasítás tárgyi hatálya

1.3.1 Jelen utasítás a KIFÜ minden személyes adatkezelésére és adatfeldolgozására vonatkozik, amely természetes személy személyes adatainak kezelését érinti, beleértve az adatkezelés minden elemét, függetlenül attól, hogy az elektronikusan vagy papír alapon történik.

1.4 Az utasítás személyi hatálya

1.4.1 Az utasítás hatálya a KIFÜ valamennyi szervezeti egységére, közalkalmazottjára és munkavállalójára (foglalkoztatott) kiterjed.

1.4.2 Az utasítás hatálya kiterjed továbbá - a velük kötött szerződésben és a titoktartási nyilatkozatban foglalt mértékben - a KIFÜ-vel szerződéses jogviszonyban álló természetes személyekre, jogi személyekre és egyéb szervezetekre, valamint ezek alkalmazottaira is a velük kötött polgári jogi szerződésekben meghatározott mértékben.

Ennek érdekében biztosítani kell, hogy az érintett személyek jelen utasítást a szükséges mértékben megismerjék.

1.4.3 Az utasítás elkészítéséért, aktualizálásáért a KIFÜ adatvédelmi tisztviselője felelős.

1.5 Az utasításra a hatálybalépéskor vonatkozó speciális jogszabály

1.5.1 Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR).Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.).

1.6 Kapcsolódó belső szabályzatok

1.6.1 A közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló utasítás (jelen utasítás hatályba lépésekor: 48/2018. számú utasítás);

1.6.2 A KIFÜ Egyedi Iratkezelési Szabályzatáról szóló utasítás (jelen utasítás hatályba lépésekor: 1/2019. számú utasítás);

1.6.3 Az informatikai biztonsági politikáról szóló utasítás (jelen utasítás hatályba lépésekor: 30/2018. számú utasítás);

1.6.4 Az informatikai biztonsági szabályzatról szóló utasítás (jelen utasítás hatályba lépésekor: 24/2018. számú utasítás);

1.6.5 A toborzás, kiválasztás és felvételi jóváhagyás folyamatáról és a kapcsolódó adatkezelésről szóló utasítás (jelen utasítás hatályba lépésekor: 45/2018. számú utasítás);

1.6.6 A munkaviszony, illetve a közalkalmazotti jogviszony megszűnésének, megszüntetésének folyamatáról, feladatairól szóló utasítás (jelen utasítás hatályba lépésekor: 4/2019. számú utasítás);

1.6.7 A hivatali célú vezetékes és mobiltelefonok használatáról szóló utasítás (jelen utasítás hatályba lépésekor: 35/2018. számú utasítás);

1.6.8 A KIFÜ vagyonnyilatkozat-tételi kötelezettség teljesítésének rendjéről szóló utasítás (jelen utasítás hatályba lépésekor: 19/2017. számú utasítás);

1.6.9 A KIFÜ Munkavédelmi szabályzata (jelen utasítás hatályba lépésekor: 50/2018. számú utasítás);

1.6.10 A KIFÜ Tűzvédelmi szabályzata (jelen utasítás hatályba lépésekor: 51/2018. számú utasítás).

1.6.11 Jelen utasítás a mindenkor hatályos, a KIFÜ ellenőrzési nyomvonaláról szóló utasítás (jelen utasítás hatályba lépésekor a 41/2018. számú utasítás) 2. számú mellékletében megjelölt 002. folyamatcsoportot, valamint a 023.003., a 023.004., a 027.003., a 030.003., a 031.016., a 032.004. és a 032.010. számú folyamatokat érinti. Az adatvédelmi tevékenység 039. számon, önálló folyamatként került rögzítésre.

1.7 Értelmező rendelkezések

1.7.1 Jelen utasításban alkalmazott fogalmak értelmezése a GDPR 4. cikkében foglalt meghatározásokon alapul, kiegészítve az Info tv. 3.§ 3-4., 6., 11-13., 16-17., 21., 23-24. pontokkal.

1.7.2 Az alkalmazott fogalomtárat jelen utasítás *1. számú melléklete* tartalmazza.

II. RÉSZLETES RENDELKEZÉSEK

2 ALAPELVEK

2.1 A KIFÜ, mint adatkezelő úgy tervezi meg és hajtja végre az adatkezelési műveleteket, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. A technika mindenkori fejlettségére tekintettel megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, az adatok károsodása és véletlen elvesztése, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

2.2 A KIFÜ adatkezelési tevékenysége során biztosítja a GDPR-ban meghatározott alapelvek érvényesülését, így különösen:

a) Jogszerű és tisztességes eljárás és az átláthatóság elve

b) Célhoz kötöttség elve

c) Adattakarékosság elve

d) Pontosság elve

e) Korlátozott tárolhatóság elve

f) Integritás és bizalmi jelleg elve

g) Elszámoltathatóság elve

3 AZ ADATKEZELÉS ÁLTALÁNOS SZABÁLYAI

3.1 A KIFÜ minden foglalkoztatottja polgári jogi, valamint büntetőjogi felelősséggel tartozik a feladatai teljesítése során végzett adatkezelés jogszerűségéért, jelen utasításban foglaltak betartásáért.

3.2 A foglalkoztatott felelősséggel tartozik különösen, ha

a) a feladatai teljesítése során jogszerűen megismert személyes adatot illetéktelen harmadik személy számára átadja, vagy hozzáférhetővé teszi,

b) jogosultságait nem rendeltetésszerűen használja (pl. jogosulatlan lekérdezést hajt végre), adatokat jogosulatlanul más alkalmazott vagy illetéktelen harmadik személy részére hozzáférhetővé tesz.

3.3 A KIFÜ személyes adatokat kizárólag a GDPR 6. cikkében meghatározott jogalappal kezel.

3.4 A KIFÜ adatkezelést végző foglalkoztatja és a KIFÜ megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési jogosultsággal rendelkező személyek kötelesek Titoktartási nyilatkozatot (*4. sz. melléklet*) tenni.

3.5 A KIFÜ kezelésében lévő személyes adat nyilvánosságra hozatalát törvény - az adatok körének meghatározásával - közérdekből elrendelheti. Az adatok egyéb esetben történő nyilvánosságra hozatalához az érintett hozzájárulása, különleges adat esetében írásbeli hozzájárulása szükséges. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg. Az előbbieken túl a KIFÜ-ben kezelt személyes adatok nyilvánosságra hozatala tilos.

3.6 Személyes adatokon is alapuló összesített statisztikai adatok közölhetők vagy nyilvánosságra hozhatók, amennyiben azokból nem ismerhető fel az, akire az adat vonatkozik. Az adat közlése előtt az adat közlője köteles meggyőződni arról, hogy a közölt adatok alapján nem lehetséges természetes személyek azonosítása.

3.7 Az adatkezelési cél megszűnését követően az adatok törlésére az adatot ténylegesen kezelő foglalkoztatott gondoskodni köteles. A törlést az adatgazda, valamint az adatvédelmi tisztviselő bármikor jogosult ellenőrizni.

3.8 Ha valamely foglalkoztatottnak tudomására jut, hogy a jogszabályban, vagy a jelen utasításban foglalt adatvédelmi vagy adatbiztonsági rendelkezéseket megsértették, vagy ennek veszélye áll fenn, az adatvédelmi tisztviselőt haladéktalanul tájékoztatja.

3.9 Az adatvédelmi tisztviselő haladéktalanul intézkedik:

a) a személyes adatok védelmi rendszerének helyreállításáról;

b) a sérelem okainak, illetve az azt elősegítő körülmények feltárásáról;

c) a mulasztásért felelős személy felelősségének tisztázásáról.

3.10 Amennyiben az adatvédelmi tisztviselő vizsgálata alapján a KIFÜ foglalkoztatottja az adatvédelmi vagy adatbiztonsági rendelkezések megsértéséért bizonyítottan felelős, az adatvédelmi tisztviselő javaslatot tesz a fegyelmi eljárás megindítására, vagy egyéb, az adott jogviszonyra irányadó szerződés vagy jogszabály alapján alkalmazandó szankció alkalmazására.

3.11 A KIFÜ-nél megvalósuló egyes adatkezelésekről az adatvédelmi tisztviselő a GDPR 30. cikkében meghatározottakra figyelemmel naprakész nyilvántartást vezet.

4 AZ ADATVÉDELMI SZERVEZET

4.1 Az elnök

4.1.1 felelős a KIFÜ adatkezelésének jogszerűségéért;

4.1.2 gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, ennek keretében

a) az adatvédelemre és adatkezelésre vonatkozó utasítást ad ki,

b) határozatlan időre adatvédelmi tisztviselőt nevez ki;

4.1.3 jogosult a KIFÜ adatkezeléseire vonatkozó döntések meghozatalára;

4.1.4 kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről;

4.1.5 részt vesz a KIFÜ magas kockázati besorolású adatvédelmi incidenseket kivizsgáló munkacsoport munkájában.

4.2 Az adatvédelmi tisztviselő

4.2.1 a KIFÜ elnökének közvetlen irányítása alatt működik, munkája során függetlenül jár el, csak a KIFÜ elnökének tartozik beszámolási kötelezettséggel.

4.2.2 feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

4.2.3 Az adatvédelmi tisztviselő feladatait

a) a GDPR 39. cikke,

b) az Infotv. 25/M. § -a,

c) a KIFÜ mindenkor hatályos Szervezeti és Működési Szabályzata,

d) a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló, mindenkor hatályos KIFÜ utasítása (jelen szabályzat megalkotásakor a 47/2018. elnöki utasítás)

tartalmazza.

4.2.4 A KIFÜ honlapján közzétett elérhetőségeken bármely érintett az adatvédelmi tisztviselőhöz fordulhat az illetékességébe tartozó kérdésben.

4.2.5 Az adatvédelmi tisztviselő gondoskodik a KIFÜ foglalkoztatottjainak megfelelő adatvédelmi és adatbiztonsági képzéséről.

4.2.6 Az adatvédelmi tisztviselő tartós távolléte (pl. betegség, szabadság) esetén a JBF főosztályvezetője gondoskodik arról, hogy a sürgős intézkedést igénylő esetekben adatvédelmi szakértelemmel rendelkező munkatárs kerüljön kijelölésre.

4.3 Az Informatikai Biztonsági Felelős (IBF)

4.3.1 az Informatikai Biztonsági Szabályzatban meghatározott feladatai teljesítése során kiemelt figyelmet szentel a személyes adatokat érintő biztonsági intézkedések megvalósításának.

4.3.2 az adatvédelmi tisztviselő bevonásával gondoskodik az informatikai megoldások kialakítása során az adatvédelem és adatbiztonság szempontjainak érvényesüléséről. Adatvédelmi incidens esetén jelen szabályzatban meghatározottak szerint részt vesz az adatvédelmi tisztviselő által létrehozott adatvédelmi munkacsoport munkájában, az incidens megoldásában.

4.4 Az adatgazdák

4.4.1 a szervezeti egységek vezetői, akik felelősek az irányításuk alá tartozó szervezeti egységek adatkezelésének jogszerűségéért, jelen utasításban foglaltak végrehajtásáért és betartásáért.

4.4.2 jogosulatlan hozzáférés vagy az adatvédelmi előírások egyéb megsértésének észlelése esetén az adatvédelmi tisztviselő egyidejű tájékoztatása mellett intézkedést tesznek annak megszüntetésére, indokolt esetben kezdeményezik a felelősségre vonási eljárás lefolytatását.

4.4.3 adatvédelmi incidens bekövetkezése esetén részt vesznek az adatvédelmi tisztviselő által összehívott munkacsoport munkájában.

4.5 Az adatkezelést végző munkatárs

4.5.1 köteles az általa kezelt, feldolgozott adatokat az IBSZ-ben meghatározottak szerinti biztonsági osztályba sorolásuk kategóriája szerint kezelni;

4.5.2 köteles az általa végzett adatfeldolgozást jogszerűen végezni;

4.5.3 köteles a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint feldolgozni, továbbá a személyes és egyéb bizalmas adatokat az adatkezelő rendelkezései szerint tárolni és megőrizni;

4.5.4 adatvédelmi incidens gyanúja esetén köteles a jelen utasítás 5.3 és 5.4 pontjai szerint eljárni.

4.5.5 Az adatkezelést végző munkatárs az adatkezelést érintő érdemi döntést nem hozhat, saját célra adatfeldolgozást nem végezhet.

5 ADATVÉDELMI INCIDENSEK KEZELÉSE

5.1 Az adatvédelmi incidens fogalmát és kockázati besorolásának rendszerét jelen utasítás *1. számú melléklete* tartalmazza.

5.2 A leggyakrabban előforduló adatvédelmi incidensek például:

- hivatali laptop vagy mobiltelefon elvesztése;
- személyes adatok nem biztonságos tárolása, továbbítása;
- ügyfél- és partnerlisták illetéktelen másolása, továbbítása;
- szerver elleni támadás;
- honlap feltörése
- jelszó nem megfelelő védelme, illetéktelen személyek hozzáférése a jelszavakhoz.

5.3 Jelen utasítás hatálya alá tartozó személy haladéktalanul, de legkésőbb egy munkanapon belül köteles jelenteni a szervezeti egysége vezetőjének és az adatvédelmi tisztviselőnek, ha adatvédelmet vagy adatbiztonságot veszélyeztető eseményt, adatvédelmi rendelkezések sérelmét vagy annak következményeit észlelik, bekövetkezését valószínűsítik, vagy ha jelen utasítás rendelkezéseinek érvényesülése bármilyen módon ellehetetlenül.

5.4 A tudomásra jutás időpontja az az időpont, amikor az észlelő személy meggyőződik egy olyan biztonsági incidens bekövetkezéséről, amelynek következtében személyes adatok kerültek veszélybe.

5.5 Az adatvédelmi tisztviselő haladéktalanul köteles gondoskodni arról, hogy a bejelentést követően rövid vizsgálattal megállapítható legyen, hogy valóban sérültek-e adatok.

5.6 A bejelentést munkaidőben telefonon majd írásban megerősítve e-mailben, munkaidőn túl e-mailben kell megtenni az adatvédelemi tisztviselő számára a honlapon közzétett telefonszámon és az adatvedelem@kifu.gov.hu e-mailcímen.

5.7 A bejelentésnek tartalmaznia kell:

a) bejelentő nevét, telefonszámát, szervezeti egységének megnevezését;

b) az incidens megnevezését, leírását.

5.8 Ha a bejelentés tárgya érinti a KIFÜ informatikai rendszerét, a bejelentést az adatvédelmi tisztviselő továbbítja az IBF felé és az eset kivizsgálásába is bevonja.

5.9 A bejelentést az adatvédelmi tisztviselő haladéktalanul értékeli.

5.10 Az adatvédelmi tisztviselő – szükség esetén – a bejelentőtől az incidensre vonatkozó, további adatokat kérhet, úgy, mint:

a) az adatvédelmi incidens helyét, időpontját;

b) az érintett adatok és személyek körét, mennyiségét;

c) egyéb lényeges körülményeket;

d) a várható hatásokat;

e) megelőzésre, következmények enyhítésére tett intézkedéseket.

5.11 Az értékelést követően az adatvédelmi tisztviselő az incidenst kivizsgálja, ennek során

5.11.1 alacsony szintű adatvédelmi incidens esetén:

a) legkésőbb a tudomásszerzéstől számított 72 órán belül az Informatikai Biztonsági Felelőssel és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,

b) az adatvédelmi incidenst rögzíti az adatvédelmi incidensek nyilvántartására szolgáló incidensnaplóba (*5. számú melléklet*);

5.11.2 közepes szintű adatvédelmi incidens esetén:

a) haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben rajta kívül részt vesz az Informatikai Biztonsági Felelős, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és a KIFÜ elnöke,

b) a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,

c) az adatvédelmi incidenst rögzíti az adatvédelmi incidensek nyilvántartására szolgáló incidensnaplóba (*6. számú melléklet*),

d) a tudomásszerzéstől számított 72 órán belül értesíti a Hatóságot az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár bármely érintett jogaira és szabadságaira nézve.

5.11.3 magas szintű adatvédelmi incidens esetén:

a) haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben rajta kívül részt vesz az Informatikai Biztonsági Felelős, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és a KIFÜ elnöke,

b) a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről,

c) az adatvédelmi incidenst rögzíti az adatvédelmi incidensek nyilvántartására szolgáló incidensnaplóba,

d) szükség esetén értesíti a Hatóságot az adatvédelmi incidensről.

5.12 Bejelentés a Hatóság felé

5.12.1 A bejelentést az adatvédelmi tisztviselő a Hatóság által működtetett Incidens Bejelentő Rendszeren keresztül, a tudomásszerzéstől számított 72 órán belül köteles megtenni. Ha a bejelentés 72 órán belül nem történik meg, mellékelni kell a késedelem igazolására szolgáló indokokat is.

5.12.2 Nem kötelező az incidens bejelentése, amennyiben annak értékelése során az adatvédelmi tisztviselő vagy az adatvédelmi munkacsoport úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira. Ennek alátámasztása érdekében a kockázatelemzés főbb szempontjait és eredményét dokumentálni kell.

5.13 Az érintettek tájékoztatása

5.13.1 Magas szintű kockázati besorolású incidens esetén a KIFÜ adatkezelést végző foglalkoztatottja - indokolatlan késedelem nélkül, írásban (e-mailben) - köteles tájékoztatni az érintett(ek)et az adatvédelmi incidens bekövetkezéséről.

5.13.2 E tájékoztatás a mellőzhető, amennyiben

a) az adatkezelő megfelelő szervezési és védelmi intézkedéseinek következtében illetéktelenek számára értelmezhetetlenek az adatok; vagy

b) az incidenst követően adatkezelő intézkedései elhárítják a további magas kockázatot; vagy

c) a tájékoztatás aránytalan erőfeszítést követelne meg adatkezelő részéről, ilyen esetben nyilvánosan közétett információk útján, vagy egyéb hasonló módon (pl. sajtóközlemény) is megvalósulhat a tájékoztatás.

5.13.3 A tájékoztatásnak az adatvédelmi incidens bekövetkezésén kívül tartalmaznia kell:

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

b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) a KIFÜ által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

5.14 Az adatvédelmi incidensek nyilvántartása (Incidensnapló)

5.14.1 Az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekről nyilvántartást vezet, amely az adatvédelmi incidenssel érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat tartalmazza. (*5. számú melléklet*)

5.15 A szervezet adatvédelmi tudatosságának növelése

5.15.1 Az adatvédelmi tisztviselő az adatvédelmi tudatosság növelése céljából gondoskodik adatvédelmi incidensekkel kapcsolatos oktatásról, amelynek keretében a bekövetkezett adatvédelmi incidensek tapasztalatait, illetve a lehetséges adatvédelmi incidensek veszélyeit ismerteti, és a kockázatok csökkentésével, megelőzésével kapcsolatosan ad tájékoztatást.

6 HATÁSVIZSGÁLAT

6.1 Amennyiben az adatkezelés a természetes személyek jogaira és szabadságaira valószínűsíthetően magas kockázatot jelent, annak megkezdése előtt az adatkezelést végző foglalkoztatott köteles hatásvizsgálatot lefolytatni. A kockázatok értékelése során különös tekintettel kell lenni az adatkezelés céljára, jellegére, hatókörére és körülményeire.

6.2 Az adatkezeléseket érintő döntések meghozatala előtt, a hatásvizsgálat szükségességének megítélése kapcsán ki kell kérni az adatvédelmi tisztviselő véleményét, illetve biztosítani kell részvételét a döntés-előkészítő értekezleteken és a hatásvizsgálat munkafolyamataiban.

6.3 A hatásvizsgálatot szükség esetén, de legalább az adatkezelési kockázati szint változásakor újra le kell folytatni annak érdekében, hogy a személyes adatok kezelése a hatásvizsgálatban foglaltaknak megfelelően történjen.

6.4 Az adatkezelést végző foglalkoztatott a szükséges hatásvizsgálatot a GDPR 35-36. cikkében, valamint a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport (WP) 2017/248. iránymutatásában foglalt módszertani ajánlás figyelembe vételével folytatja le.

6.5 Jelen utasítás kiadásának időpontjában a KIFÜ meglévő adatkezelési folyamatai nem igénylik adatvédelmi hatásvizsgálat lefolytatását.

7 ADATBIZTONSÁG

7.1 A KIFÜ elnöke az Iratkezelési Szabályzatban – az Informatikai Biztonsági Szabályzattal összhangban – meghatározza, az iratkezelés során a foglalkoztatottakat megillető jogosultságokat, a jogosultság igénylésének és dokumentálásának módját.

7.2 A KIFÜ a foglalkoztatottaktól megköveteli, hogy a napi munkavégzés befejezésével a foglalkoztatott úgy hagyhatja el munkaállomását, hogy az általa kezelt adathordozókat elzárja.

7.3 Informatikai nyilvántartások védelme

7.3.1 A helyi számítógépeken (asztali számítógép, laptop, tablet, okostelefon) és az informatikai hálózatokon tárolt személyes adatok biztonsága érdekében, a hatályos Informatikai Biztonsági Politikájával és Informatikai Biztonsági Szabályzatával összhangban az alábbi intézkedéseket kell alkalmazni:

a) helyi számítógépre adatmentés nem végezhető, a személyes adatokat tartalmazó dokumentumokat, nyilvántartásokat stb. központi szerverekre (PMSZ, fileszerver stb.) kell menteni.

b) az adatokkal történő minden művelet (hozzáférés, felvitel, módosítás, törlés, továbbítás) nyomon követhetően naplózásra kerül;

c) a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak a megfelelő jogosultsággal rendelkező és arra kijelölt személyek férhetnek hozzá;

d) Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papírok megsemmisítési szabályai irányadóak.

7.3.2 Az informatikai nyilvántartások biztonságát a KIFÜ adatkezelést végző foglalkoztatottjai az alábbi garanciális elemek alkalmazásával fokozzák:

a) a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval - lehet csak hozzáférni, a jelszavak cseréjéről rendszeresen, illetve indokolt esetben soron kívül gondoskodni kell;

b) amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot visszaállíthatatlanul törölni kell;

c) a hálózaton tárolt adatok biztonsága és az adatvesztés elkerülése érdekében a szerveren folyamatos adatmentést kell végezni;

d) a személyes adatokat tartalmazó adatbázisok aktív adatairól a központi szerver teljes adatállományára vonatkozóan naponta adatmentést kell végezni;

e) a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodni kell;

f) illetéktelen személyek hálózati hozzáférését a rendelkezésre álló számítástechnikai eszközök alkalmazásával meg kell akadályozni.

7.4 Szerverek biztonsága

7.4.1 A személyes adatok tárolásának helyén, a szerverszobákban tárolt szerverek fizikai védelme érdekében a KIFÜ az alábbi intézkedéseket alkalmazza:

a) Mind a központosított adattárolók, mind pedig a szerverek külön erre a célra kialakított helyiségekben kerülnek elhelyezésre. Ezen helyiségekre vonatkozóan a KIFÜ Informatikai Biztonsági Szabályzatában (IBSZ), valamint az Iratkezelési Szabályzatban meghatározottak szerint alakít ki hozzáférési jogosultsággal rendelkező foglalkoztatotti-bázist, akik engedéllyel férhetnek hozzá ezekhez az eszközökhöz és esetlegesen a rajtuk tárolt adatokhoz.

b) Azon helyiségekre vonatkozóan, ahol szervergépek, központi adattárak, biztonsági mentéseket végrehajtó és egyéb érzékeny adatokat tároló informatikai eszközök kerülnek elhelyezésre a KIFÜ az IBSZ-ben fizikai védelmi eljárásrendet alakít ki, meghatározza a biztonsági zónák kategóriáit.

c) A szerverszoba klimatizált és tűzoltó berendezéssel ellátott helyiség, a tűzvédelmi előírásokat a KIFÜ mindenkor hatályos tűzvédelmi szabályzata tartalmazza.

d) Az IBSZ-ben meghatározottak szerint az informatikai rendszerek szempontjából kiemelt fontosságú helyiségekbe csak külön beléptető rendszer útján, az arra jogosultaknak lehet bejutni.

e) Az IKT üzemeltetési vezető szúrópróbaszerűen átvizsgálja a fizikai hozzáférésekről készült naplókat. Ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak, soron kívül átvizsgálja a fizikai hozzáférésről készült naplókat és intézkedik a megfelelő reagálásról.

f) A KIFÜ az általa kezelt személyes adatok áramlását elsősorban elektronikus módon, szerverek segítségével, fizikai tárolásukat pedig adattárolók segítségével valósítja meg.

7.5 Papíralapú nyilvántartások védelme

7.5.1 A papír alapú adatok biztonsága vonatkozásában a KIFÜ mindenkor hatályos Iratkezelési Szabályzatában foglaltak az irányadók.

7.5.2 A KIFÜ a papíralapú nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság és tűzvédelem tekintetében.

7.5.3 A foglalkoztatottak és más, a KIFÜ érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

7.5.4 Az iratkezelés felügyeletére a KIFÜ elnöke az Iratkezelési Szabályzatban foglaltak szerint kijelöli az iratkezelés felügyeletéért felelős asszisztenst (a továbbiakban: IKA).

7.5.5 A papíralapon kezelt személyes adatok biztonsága érdekében a KIFÜ az alábbi intézkedéseket alkalmazza:

a) az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára nem tárhatók fel;

b) a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;

c) biztosítja, hogy a folyamatos, aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;

d) Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, a KIFÜ intézkedik a selejtezéséről, valamint a megsemmisítéséről az Iratkezelési Szabályzatban foglaltaknak megfelelően. A selejtezésről jegyzőkönyv készül (a mindenkor hatályos iratkezelési szabályzat melléklete, jelen utasítás hatályba

lépésekor az 1/2019. KIFÜ utasítás 8. számú melléklete), amelyet a Magyar nemzeti Levéltár záradékol. Ez alapján a megsemmisítésre váró iratok az Iratkezelési Szabályzatban foglaltaknak megfelelően a selejtezési iratjegyzékkel (a mindenkor hatályos iratkezelési szabályzat melléklete, jelen utasítás hatályba lépésekor az 1/2019. KIFÜ utasítás 9. számú melléklete) ellátva a megsemmisítésig az IKA intézkedésére tárolásra kerülnek. A megsemmisítésre a KIFÜ külső céget vehet igénybe.

7.6 Jogosultságkezelés

7.6.1 Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell. A jogosultság kezelés célja, hogy a kiosztott jogosultságok naprakészen, pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen.

7.6.2 A személyes adatok biztonsága érdekében a KIFÜ a jogosultságkezelési szabályzatában az alábbi jogosultságkezelési alapelveket alkalmazza:

a) Új jogosultság beállítását, illetve jogosultság megváltoztatását az adatgazda felhatalmazása alapján rendszergazda végzi.

b) A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani, el kell kerülni, hogy a felhasználók teljes hozzáférést vagy adminisztrátori jogosultságokat kapjanak.

c) Adminisztrátori jogosultsággal rendelkező, nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az IKT üzemeltetési vezető engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.

d) Nem KIFÜ foglalkoztatott folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

e) Jogosultságigényléshez, -módosításhoz az IKT üzemeltetési vezetőnek, jelen szabályzat *6. számú mellékletének* megfelelő tartalmú, aláírt, vagy informatikai rendszerben azonosított jogosultságigényt kell küldeni.

7.7 Titoktartási kötelezettség

7.7.1 A KIFÜ-vel közalkalmazotti jogviszonyt, munkavégzésre irányuló egyéb jogviszonyt létesítő vagy egyéb szerződést (így különösen megbízási, vállalkozási szerződést) kötő személy vagy szervezet üzleti titokként köteles megőrizni a tevékenysége ellátásával kapcsolatban tudomására jutott minden olyan adatot, tényt vagy körülményt, amelyet törvény előírásai szerint a KIFÜ nem köteles más hatóság, illetve a nyilvánosság számára hozzáférhetővé tenni. A megőrzési kötelezettség a jogosulatlan közzététel és a hasznosítás tilalmát is jelenti.

8 AZ ÉRINTETTEK JOGAI

8.1 Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve a jogszabály által elrendelt adatkezelések kivételével adatainak törlését, vagy kezelésük korlátozását, tiltakozhat a személyes adatainak kezelése ellen a GDPR 13-22. cikkében foglaltaknak megfelelően.

8.2 A KIFÜ foglalkoztatottjai az érintettek jogainak biztosítása során jelen utasítás 3. fejezetében foglaltakkal összhangban járnak el.

8.3 Tájékoztatáshoz való jog

8.3.1 Az előzetes tájékozódáshoz való jog

a) A KIFÜ adatkezelést végző munkatársa az adatkezelés megkezdése előtt minden esetben tájékoztatja az érintettet az adatkezelés céljáról és jogalapjáról, valamint a GDPR 13. cikkében foglalt tartalommal adatkezelési tájékoztatót készít és tesz elérhetővé. A tájékoztatót és annak esetleges módosításait az adatkezelést végző munkatárs készíti el, és jóváhagyásra megküldi az adatvédelmi tisztviselő részére. Az adatkezelési tájékoztató elérhetővé tétele előtt az adatkezelés nem kezdhető meg.

b) Az adatkezelési tájékoztatót a KIFÜ adatkezelést végző munkatársa az érintettek rendelkezésére bocsájtja, valamint intézkedik a KIFÜ honlapján való közzétételről. Az adatkezelési tájékoztató sablonját a *2. számú melléklet* tartalmazza.

c) Az adatkezelési tájékoztató minimális tartalmára a GDPR 13.-14. cikkében foglaltak az irányadók.

8.3.2 A hozzáféréshez való jog (tájékoztatás az érintett kérelmére)

a) Az érintettnek a KIFÜ által végzett adatkezelések kapcsán joga van ahhoz, hogy a KIFÜ által tárolt személyes adatait és a kezelésükkel kapcsolatos információkat megismerhesse, bármikor kikérje, ellenőrizze, hogy a KIFÜ milyen személyes adatait kezeli.

b) Hozzáférési jog gyakorlása esetén az érintett az alábbi információkról kérhet tájékoztatást:

- a kezelt adatok köre,
- az adatkezelés célja, ideje, jogalapja,
- történik-e vagy fog-e történi adattovábbítás és kinek a részére,
- az adatok tárolásának tervezett időtartama, vagy ezen időtartam meghatározásának szempontjai,
- a tárolt adatok helyesbítésének, törlésének, kezelés korlátozása kérelmezésének joga, adatok kezelésével kapcsolatos tiltakozás joga,
- adatforrás megjelölése, amennyiben nem az érintettől gyűjtötték,
- harmadik ország, vagy nemzetközi szervezet részére történő adattovábbítás ténye, a továbbítás garanciái.

c) Az érintett az adatokhoz való hozzáférésre irányuló kérelmét az erre a célra szolgáló formanyomtatványon (*7. számú melléklet*), írásban köteles eljuttatni a KIFÜ részére és az igényelt tájékoztatást a KIFÜ kizárólag írásban (elektronikusan vagy postai úton küldött levélben) adja meg. A formanyomtatványok a KIFÜ honlapján az adatvédelmi felület letölthető dokumentumai között elérhetők.

d) Az érintett a tájékoztatást követően, amennyiben az adatkezeléssel, a kezelt adatok helyességével nem ért egyet, úgy az alábbiakban meghatározottak szerint kérelmezheti a rá vonatkozó adatok helyesbítését, kiegészítését, törlését, kezelésének korlátozását, tiltakozhat az adatok kezelése ellen, valamint a 8.4 – 8.8 pontokban meghatározott eljárást kezdeményezhet.

8.4 Kezelt személyes adatok helyesbítéséhez, kiegészítéséhez való jog

8.4.1 Az érintett kérelmére a KIFÜ adatkezelést végző munkatársa indokolatlan késedelem nélkül helyesbíti az érintett által, írásban megjelölt pontatlan személyes adatokat, illetve - az adatkezelés célját szem előtt tartva - a hiányos adatok kiegészítését elvégzi az érintett által megjelölt tartalommal. A helyesbítés tényéről a KIFÜ adatkezelést végző munkatársa köteles tájékoztatni mindenkit, akinek az érintett adatot továbbította, átadta, megosztotta.

8.4.2 A személyes adatok helyesbítését vagy kiegészítését az érintett az erre a célra szolgáló formanyomtatvány (*8. számú melléklet*) benyújtásával kezdeményezheti.

8.5 A törléshez való jog

8.5.1 A KIFÜ adatkezelést végző munkatársa az alábbi esetekben haladéktalanul köteles törölni az adatokat:

a) ha az adatkezelésének célja megvalósult és már nincs szükség az adatok további kezelésére;

b) az érintett a hozzájárulását visszavonta és más jogalap nem támasztja alá az adatkezelés jogszerűségét;

c) az érintett tiltakozik a személyes adatai kezelése ellen a GDPR 21. cikk (1)-(2) bekezdésekben meghatározott egyes automatizált döntéshozatali ügyek esetében;

d) az adatok kezelése jogellenes;

e) az adatokat az adatkezelőre vonatkozó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölnie kell;

f) az adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálása céljából került sor.

8.5.2 A KIFÜ adatkezelést végző munkatársa a törlést illetően minden rendelkezésre álló technikai eszközt felhasznál, hogy a törlés teljes körű legyen (linkek, másolatok, másodpéldányok törlése, további adatkezelők, adatfeldolgozók, címzettek tájékoztatása a törlés tényéről).

8.5.3 Az érintett törléshez való jogának érvényesítése korlátozható, amennyiben az adatkezelés az alábbi okokból szükséges:

a) az adatkezelés szükséges a véleménynyilvánítás szabadságához és a tájékoztatáshoz való jog gyakorlása céljából;

b) európai uniós vagy tagállami jog teljesítése miatt, közérdekből végzett közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;

c) egyes népegészségügy területét érintő közérdek alapján;

d) közérdekű archiválás céljából, tudományos vagy történelmi kutatási célból, statisztikai célból, ha a törlés ezen feladatok megvalósítását komolyan veszélyeztetné;

e) jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez.

8.5.4 Az adatok törléséhez való jogát az érintett az erre a célra szolgáló formanyomtatvány (*9. számú melléklet*) benyújtásával kezdeményezheti.

8.6 Adatkezelés korlátozásához való jog

8.6.1 Az érintett jogosult arra, hogy írásbeli kérelme esetén a KIFÜ, mint adatkezelő korlátozza az adatkezelést, ha

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a KIFÜ adatkezelést végző munkatársa ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, az érintett az adatok törlését ellenzi és ehelyett azok felhasználásának korlátozását kéri;

c) a KIFÜ-nek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez igényli;

d) az érintett tiltakozik az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a KIFÜ jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

8.6.2 A korlátozás időtartama alatt ezen adatokat a tároláson kívül KIFÜ csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez, vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelmében, vagy fontos közérdekből kezelheti.

8.6.3 A KIFÜ adatkezelést végző munkatársa az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja azt az érintettet, akinek kérelmére az adatkezelést korlátozta.

8.7 Adathordozhatósághoz való jog

8.7.1 Az adathordozhatóság azt teszi lehetővé, hogy az érintett megszerezhesse, és a továbbiakban felhasználhassa a KIFÜ rendszerében megtalálható általa átadott „saját" adatait, továbbá ezeket az adatokat egy másik adatkezelőnek továbbítsa. Minden esetben az érintett által átadott adatokra korlátozódik a jogosultság, egyéb adatok hordozhatóságára lehetőség nincs. (pl. statisztika, tranzakciós adatok stb.)

8.7.2 Az érintett a rá vonatkozó, a KIFÜ rendszerében megtalálható adatokat:

a) tagolt, széles körben használt, géppel olvasható formátumban megkapja,

b) jogosult más adatkezelőhöz továbbítani,

c) kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz, ha ez technikailag megvalósítható a KIFÜ rendszerében.

8.7.3 Az adathordozhatóság joga kizárólag abban az esetben illeti meg az érintettet, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon, gépi eszközzel történik.

8.8 Tiltakozás személyes adatok kezelése ellen

8.8.1 Az érintett a saját helyzetével kapcsolatos okokból írásban tiltakozhat adatainak kezelése ellen, ideértve a profilalkotást is, továbbá az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok közvetlen üzletszerzés célból történő kezelése ellen, ideértve a profilalkotást is.

8.8.2 A tiltakozás joga csak abban az esetben illeti meg az érintettet, ha az adatkezelés közérdekből vagy közhatalmi jogosultság gyakorlása keretében végzett feladat végrehajtásához, illetve az adatkezelő vagy egy harmadik fél jogos érdekei alapján szükséges. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

8.9 Ha az érintett úgy ítéli meg, hogy a KIFÜ a személyes adatainak kezelése során megsértette a hatályos adatvédelmi követelményeket, akkor

8.9.1 panaszt nyújthat be a Hatósághoz, vagy

8.9.2 lehetősége van adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el.

9 A JOGÉRVÉNYESÍTÉSRE VONATKOZÓ KÉRELMEK TELJESÍTÉSÉNEK SZABÁLYAI

9.1 A kérelem benyújtása elsősorban a formanyomtatványok kitöltésével történhet.

9.2 A kérelmet a KIFÜ adatvédelmi tisztviselője megvizsgálja, hogy annak tartalmi elemei elégségesek-e az adatszolgáltatási folyamat megindításához.

9.2.1 A KIFÜ honlapján közzétett formanyomtatvány kitöltésétől el lehet tekinteni és az kérelem teljesítésének folyamatát meg lehet indítani, ha a kérelmező által benyújtott adatigénylés tartalmazza

a) a kérelmező beazonosításához szükséges információkat,

b) az adatkezeléssel közvetlenül összefüggő, az érintett és a KIFÜ között létrejött jogviszony, vagy az érintett által igénybe vett szolgáltatás megnevezése,

c) a kérelmező elérhetőségét (értesítési cím, telefonszám, e-mailcím),

d) a személyes adatok kezelésével kapcsolatban érvényesíteni kívánt jog pontos meghatározását,

e) a kérelmező nyilatkozatát arra, hogy a választ milyen formában szeretné és melyik elérhetőségére megkapni (elektronikus, postai, egyéb)

9.2.2 Amennyiben a kérelem a 9.4.1 pont a-e) alpontjaiban foglalt elemek valamelyikét egyáltalán nem, vagy annyira hiányosan tartalmazza, hogy abból az érvényesíteni kívánt jog tartalma nem válik egyértelművé, a KIFÜ adatvédelmi tisztviselője a kérelem beérkezésétől számított 3 napon belül, az abban megjelölt elérhetőségen felhívja az érintettet a kérelem pontosítására.

9.3 A formanyomtatványok formai és tartalmi frissítéséért a KIFÜ adatvédelmi tisztviselője, a KIFÜ honlapján történő közzétételéért pedig a Koordinációs Főosztály (a továbbiakban: KOF) felelős.

9.4 A KIFÜ-höz beérkezett kérelmet a KOF Elnöki Titkárság (a továbbiakban: KOF ET) a mindenkor hatályos iratkezelési szabályzatnak megfelelően iktatja, majd haladéktalanul, de legkésőbb a beérkezést követő munkanapon, szkennelt formában megküldi a KIFÜ adatvédelmi tisztviselőjének.

9.5 A kérelem kezelésének általános szabályai

9.5.1 A KIFÜ az érintett adatvédelemmel kapcsolatos jogainak érvényesítésére irányuló kérelemének a lehető legrövidebb idő alatt, de legfeljebb 1 hónapon belül eleget tesz. Az e tárgykörben felmerült határidők számítására a GDPR 12. cikkének rendelkezései az irányadóak.

9.5.2 A KIFÜ adatvédelmi tisztviselője a kérelem kézhezvételét követő 2 munkanapon belül értesíti a kérelemről az adatkezeléssel érintett szervezeti egység vezetőjét, mint adatgazdát, és bekéri a kérelem elbírálásához szükséges információkat.

9.5.3 Az adatgazda ezt követően 5 munkanapon belül megküldi az adatvédelmi tisztviselőnek a kért információkat. A kérelem összetettségére való tekintettel az adatgazda a GDPR 12. cikk (3) bekezdés szerint a teljesítés határidejének további, legfeljebb 2 hónappal történő meghosszabbítását javasolhatja az adatvédelmi tisztviselő felé. Amennyiben a kérelemben foglaltak teljesítése kimutathatóan aránytalan dologi és/vagy személyi jellegű költséggel (papír/adathordozó költsége, aránytalan mértékű munkaerő-ráfordítás) jár, ennek mértékéről az adatgazda tételes kimutatást (a továbbiakban: költségkimutatás-tervezet) készít, amelyet szintén megküld a KIFÜ adatvédelmi tisztviselőjének.

9.5.4 Amennyiben a kérelem nem teljesíthető, a KIFÜ adatvédelmi tisztviselője jogszabályi indokolást és a jogorvoslati lehetőségekről való tájékoztatást is tartalmazó válaszlevelet készít, amelyet – az elnök általi aláírás és az érintettnek történő továbbítás céljából – haladéktalanul megküld a KOF ET részére.

9.5.5 Amennyiben a kérelem teljesíthető, a KIFÜ adatvédelmi tisztviselője utasítására az adatgazda 5 munkanapon belül intézkedik a kérelemben foglaltak teljesítésére, és ennek megtörténtéről az adatvédelmi tisztviselőt elektronikus levélben értesíti.

9.5.6 Amennyiben a kérelem által érintett adatkezelés során adattovábbítás történt, a KIFÜ adatkezelést végző munkatársa köteles gondoskodni arról, hogy a kérelemben foglaltak az adattovábbítás címzettjeinél is érvényre jussanak.

9.5.7 A KIFÜ adatvédelmi tisztviselője az adatgazdától kapott értesítés alapján gondoskodik az érintettnek küldendő, jogszabályi indokolást és a jogorvoslati lehetőségekről szóló tájékoztatást is tartalmazó válaszlevél elnöki aláírásra történő előkészítéséről.

9.5.8 Az kérelmezőnek írt válaszlevelet az elnök általi aláírást követően a KOF ET a mindenkor hatályos iratkezelési szabályzatnak megfelelően iktatja, majd megküldi a kérelmező által megadott elérhetőségre.

9.6 Az kérelem teljesítésének speciális szabályai

9.6.1 Amennyiben az adatgazda a kérelem összetettségére (vagy a kérelmek mennyiségére) való tekintettel a teljesítés határidejének meghosszabbítását javasolja, az adatvédelmi tisztviselő a kérelem beérkezésétől számított 30 napon belül az érintettnek címzett, a meghosszabbítás tényéről és indokairól, valamint az esetlegesen felmerülő költségekről szóló tájékoztató levelet készít, amelyet az elnök általi aláírást követően a KOF ET a mindenkor hatályos iratkezelési szabályzatnak megfelelően iktat, majd megküld a kérelmező által megadott elérhetőségre.

9.6.2 A költségtérítésnek a kérelmező általi befizetését követően az eljárás az általános szabályok szerint, a 9.5.5 pontban foglaltaknak megfelelően folytatódik.

10 ELLENŐRZÉS

10.1 Az adatvédelemmel kapcsolatos jogszabályi előírások és belső szabályozási dokumentumok betartását az adatkezelést végző szervezeti egységek vezetői (adatgazdák) jogosultak és kötelesek folyamatosan ellenőrizni jelen szabályozás alapján.

10.2 A KIFÜ adatvédelmi tisztviselője jogosult általános és célellenőrzéseket végezni. Az ellenőrzés megkezdéséről a belső ellenőrzési vezetőt – az ellenőrzés megkezdéséig, vagy azzal egyidejűleg – tájékoztatni köteles.

10.3 Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

a) a foglalkoztatottak belépési, valamint betekintési és hozzáférési jogosultságának naprakészsége,

b) a fizikai biztonsági előírások érvényesülése (elektronikus beléptető rendszer, riasztó rendszer),

c) tűzvédelmi szabályok betartása,

d) jelszavak időnkénti cseréje,

e) az adattovábbítási nyilvántartás vezetése,

f) az adathordozók meglétének szúrópróbaszerű ellenőrzése,

g) selejtezés, megsemmisítés végrehajtása, dokumentálása,

h) jelen utasítás rendelkezéseinek betartása.

10.4 Az ellenőrzésre feljogosított az ellenőrzés céljára figyelemmel az ellenőrzés érdekében minden olyan helyiségbe beléphet, ahol adatkezelés folyik, az adatkezelést végzőktől minden olyan kérdésben felvilágosítást kérhet, minden olyan adatkezelést megismerhet, vagy abba betekinthet, amely az ellenőrzött szerv adatkezelési tevékenységével összefügg.

10.5 Az adatvédelmi tisztviselő jogosult az irat és adatkezeléssel kapcsolatos belső szabályozási dokumentumok, jegyzőkönyvek és nyilvántartások áttekintésével ellenőrizni az adatkezelés törvényes rendjének megtartását. Törvénysértés esetén annak megszüntetésére szólítja fel az

adatkezelő személyt vagy szervezeti egység vezetőjét, különösen súlyos jogszabálysértés esetén pedig az elnökhöz fordul.

10.6 Az adatvédelmi tisztviselő jogosult a személy és munkaügyi nyilvántartások rendszerét ellenőrizni.

11 A HATÓSÁG VIZSGÁLATÁBAN VALÓ KÖZREMŰKÖDÉS

11.1 A KIFÜ az adatvédelmi tisztviselője útján együttműködik a Hatósággal, a Hatóság kérésének a megállapított határidőn belül eleget tesz, illetve amennyiben a Hatóság által tett megállapításokkal, illetve a Hatóság által meghatározott határozatokkal nem ért egyet, megteszi a szükséges és lehetséges lépéseket.

12 AZ ADATTOVÁBBÍTÁS SZABÁLYAI

12.1 Adatok továbbítására kizárólag jogszabály felhatalmazása, vagy az érintett hozzájárulása alapján kerülhet sor.

12.2 Az adattovábbítást megelőzően a KIFÜ adatkezelést végző munkatársa ellenőrzi a továbbítandó adatok naprakészségét, pontosságát és teljességét, valamint az adattovábbítás feltételeinek meglétét.

12.3 KIFÜ-n belüli adattovábbítás során a személyes adatokat kezelő munkatárs köteles körültekintően eljárni, csak olyan munkatársnak küldheti tovább az adatokat, akinek azok kezelésére jogosultsága van. Az adott adatcsoportok útját minden esetben nyomon kell tudni követni.

12.4 A harmadik fél felé történő adattovábbítás esetén az adattovábbítást minden esetben írásban dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen. Az egyes adatkezelésekhez készült adatkezelési tájékoztatóban tájékoztatni kell az érintetteket az adattovábbítások tényéről és címzettjeiről. Az adattovábbítás előtt az adatkezelést végző munkatárs tájékoztatja az adatvédelmi tisztviselőt az adattovábbítás lényeges jellemzőiről (a kezelt adatok továbbításának módja és időpontja, a továbbított adatkörök, az adattovábbítás jogalapja, az adattovábbítás címzettje, az adattovábbításért felelős neve és elérhetősége) szükség esetén kikéri álláspontját. Az adattovábbításokról az adatvédelmi tisztviselő naprakész nyilvántartást vezet.

12.5 Jogszabályon alapuló adatszolgáltatási kötelezettség teljesítése

12.5.1 A KIFÜ adatot jogszabályban meghatározott szerv, vagy személy részére és adatkörben a célhoz kötöttség elvének maradéktalan érvényesítésével szolgáltathat.

12.5.2 Jogszabályban meghatározott adatszolgáltatási kötelezettség esetén a KIFÜ adatkezelést végző munkatársa minden esetben ellenőrzi az adatkezelés jogalapjának meglétét. A KIFÜ csak olyan személyes adatot továbbíthat, amelynek a KIFÜ a törvényben meghatározott adatkezelője.

12.5.3 A fentieken túl adatot továbbítani csak akkor lehet, ha ahhoz az érintett egyértelműen és dokumentálhatóan hozzájárult. Az érintettek hozzájárulásához kötött adattovábbítás esetén az érintett a nyilatkozatát az adattovábbítás címzettje és célja ismeretében adja meg.

12.6 Adattovábbítás kérelem alapján

12.6.1 Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása - a törvényben kötelezően előírt adattovábbítás esetét kivéve - a KIFÜ elnökének hatáskörébe tartozik, a kérelem megválaszolása az adatvédelmi tisztviselő állásfoglalásának figyelembe vételével történik.

12.6.2 Az adattovábbítási kérelem abban az esetben teljesíthető, ha az tartalmazza:

a) az adattovábbítás célját, jogalapját (az alapul szolgáló törvényi rendelkezés pontos megjelölését);

b) a kért adatok körének pontos meghatározását;

c) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

12.6.3 Ha az adattovábbítási kérelem olyan adatra vonatkozik, amely esetében más az adatkezelő és a KIFÜ csak adatkérésre jogosult, a kérelmet – jogszabály kifejezetten eltérő rendelkezése hiányában – a KIFÜ elutasítja és a kérelmezőt tájékoztatja arról, hogy a kért adatokat mely adatkezelőtől igényelheti.

12.7 Adattovábbítás az adatfeldolgozó részére

12.7.1 A KIFÜ csak olyan adatfeldolgozót vehet igénybe, amely megfelelő garanciákat nyújt az adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtására és az adatkezelés biztonságára.

12.7.2 Adatfeldolgozó igénybevétele esetén az adatkezelés körülményeiről, az adatkezelés céljáról, idejéről, a kezelt adatok köréről, az átadás módjáról és az adatátadás, valamint az adatfeldolgozó adatkezelési garanciáinak részleteiről a szerződésben rendelkezni kell, vagy külön adatfeldolgozói megállapodást (*3. számú melléklet*) kell kötni.

12.7.3 A KIFÜ adatvédelmi tisztviselője köteles a gondoskodni arról, hogy az adatfeldolgozóval kötött szerződés az adatok védelmének jogszabályi garanciáit megfelelően tartalmazza, valamint az adatfeldolgozó a tevékenysége során betartsa a KIFÜ vonatkozó belső utasításait.

12.7.4 A KIFÜ által igénybe vett adatfeldolgozókról a KIFÜ adatvédelmi tisztviselője nyilvántartást vezet.

III. VEGYES RENDELKEZÉSEK

13 ZÁRÓ RENDELKEZÉSEK

13.1 A hatályt érintő rendelkezések

13.1.1 A jelen utasítás a közzétételt követő munkanapon lép hatályba és visszavonásig hatályban marad.

13.1.2 Az utasítás hatálybalépésével egyidejűleg hatályát veszti a KIFÜ adatvédelmi és adatbiztonsági szabályzatáról szóló 34/2017. számú KIFÜ utasítás.

13.2 Technikai rendelkezések

13.2.1 A jelen utasításról folyamatábra nem készült, folyamatkezelő rendszerrel nem támogatott.

13.2.2 A jelen utasításról rövid összefoglaló készül.

13.3 Mellékletek, függelékek

13.3.1 Jelen utasításhoz a Tudástárban az alábbi dokumentumok kapcsolódnak:

a) *1. számú melléklet*: Adatvédelmi fogalomtár

b) *2. számú melléklet*: Adatkezelési tájékoztató (sablon)

c) *3. számú melléklet*: Adatfeldolgozási megállapodás (sablon)

d) *4. számú melléklet*: Titoktartási nyilatkozat (sablon)

e) *5. számú melléklet*: Incidensnapló – incidens nyilvántartó lap (sablon)

f) *6. számú melléklet*: Jogosultságkezelési megrendelőlap (sablon)

g) *7. számú melléklet*: Tájékoztatás kérése (sablon)

h) *8. számú melléklet*: Helyesbítési kérelem (sablon)

i) *9. számú melléklet*: Törlési kérelem (sablon)

Budapest, 2019. május „ 24. ”

Szijártó Zoltán
elnök