ÁEEK
Állami Egészségügyi Ellátó Központ
1125 Budapest, Diós árok 3.
Tel.: 1 356 1522, Fax: 1 375 7253
1525 Budapest 114 Pf. 32.

32/2018. számú Főigazgatói Utasítás

Tárgy: Adatvédelmi és adatbiztonsági szabályzat

1. Az Adatvédelmi és adatbiztonsági szabályzatot jelen utasítás mellékleteiben foglaltak szerint határozom meg.
2. Jelen utasítás 2018. november 26. napján lép hatályba.
3. Jelen utasítás hatálybalépésével egyidejűleg hatályát veszti a 49/2015. számú Főigazgatói utasítás.

Budapest, 2018. november „ 16 ”

Dr. Gondos Miklós
főigazgató

Jelen belső szervezetszabályozó dokumentum az ÁEEK szellemi tulajdona. Továbbadása, sokszorosítása írásos engedélyhez kötött. A dokumentumban szereplő információkat csak az ÁEEK működtetéséhez lehet felhasználni.

Állami Egészségügyi Ellátó Központ

32/2018. számú Főigazgatói utasítás
Adatvédelmi és adatbiztonsági szabályzat

Adatvédelmi és adatbiztonsági szabályzat

Dokumentum-azonosító:	32/2018.
Iktatószám:	ÁEEK/64608-2/2018.
File név:	32_Adatvedelem_adatbiztonsag
Kiadás száma:	1
Hatálybalépés időpontja:	2018. november 26.
Érvényesség:	Visszavonásig
Hatályon kívül helyezett szabályozások:	49/2015. számú Főigazgatói utasítás

Készítette: Dr Sebestyén Kálmán
Sebestyén Kálmán
adatvédelmi tisztviselő
Informatikai Igazgatóság
2018. november „26”

Jogi ellenőrző:
Dr. Szabó Garbai Dénes
igazgató
Jogi, Igazgatási és Humánpolitikai Igazgatóság
2018. november „21”

Jóváhagyta:
Jobbágy László
informatikai biztonsági felelős
2018. november „23”

Jóváhagyta:
Donauer Zsolt
igazgató
Informatikai Igazgatóság
2018. november „26”

Jóváhagyta:
Dr. Lénárt Endre
főigazgató-helyettes
Informatikai és Egészségügyi Készletgazdálkodási Főigazgatóság
2018. november „26.”

Jóváhagyta:
általános főigazgató-helyettes
Általános Főigazgatóság
2018. november „26”

Jóváhagyta:
Dr. Gondos Miklós
főigazgató
2018. november „26”

Nyilvántartott példány: ☐

E példány sorszáma: 01

Törzsnyilvántartási szám: 32/2018. Oldal: 2/16

TARTALOMJEGYZÉK

1. A SZABÁLYZAT CÉLJA

Jelen Szabályzat az Európai Parlament és a Tanács (EU) 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 5/22 rendeletének (a továbbiakban: GDPR rendelet), valamint a hazai adatvédelmi szabályozás, így különösen az Infotv. rendelkezéseinek való megfelelést szolgálja.

A Szabályzat célja továbbá, hogy az Alaptörvény VI. cikk (2) bekezdése értelmében az ÁEEK tevékenysége során biztosítsa a kezelt személyes adatok védelmét, meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat.

A Szabályzat további célja a személyes adatnak nem minősülő, de egyéb okból nem nyilvános adatok védelmének biztosítása.

2. A SZABÁLYZAT HATÁLYA

A Szabályzat hatálya kiterjed az Állami Egészségügyi Ellátó Központ (A továbbiakban: ÁEEK) valamennyi szervezeti egységére.

A Szabályzat személyi hatálya kiterjed az ÁEEK-ban foglalkoztatott valamennyi közszolgálati tisztviselőre, munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottakra, továbbá azon személyekre, akik – munkatapasztalat-szerzési, kutatási vagy képzési célból — szakmai gyakorlatukat az ÁEEK valamely szervezeti egységénél töltik (a továbbiakban együtt: Munkatársak). A Szabályzat hatálya kiterjed az ÁEEK által kezelt személyes, illetőleg különleges (egészségügyi adatok teljes körére.

Jelen Szabályzat rendelkezéseiben az ÁEEK – a jogszabály alapján ellátott, illetve egyéb átruházott feladataitól függően – adatkezelőnek, illetve adatfeldolgozónak minősül.

A Szabályzat alkalmazását elő kell írni az ÁEEK részére vállalkozási vagy megbízási szerződés keretében szolgáltatást nyújtók felé, amennyiben tevékenységük során az ÁEEK által kezelt adatokhoz hozzáférnek.

Jelen szabályzat a közérdekű adatigénylésekre nem vonatkozik.

3. FELELŐSSÉG MEGHATÁROZÁSA

Jelen szabályzatban meghatározott, szabályozott tevékenységek végrehajtásában az alábbiak illetékesek, felelősek:

A szabályzat elkészítéséért: adatvédelmi tisztviselő

A szabályzat ellenőrzéséért: informatikai biztonsági felelős, jogi igazgató

A szabályzat jóváhagyásáért: a főigazgató

A szabályzatban foglaltak alkalmazásért meghatározott feladatkörökben:

- az ÁEEK mindazon munkatársai, akiknek a jelen szabályzat személyi hatálya kiterjed

A szabályzatban foglaltak alkalmazásának ellenőrzéséért:

- a jelen szabályzatban erre feljogosított vezetők,
- a belső ellenőrök.

4. FOGALOM MEGHATÁROZÁSOK

1. Munkatárs: az ÁEEK-ban dolgozó kormánytisztviselő, kormányzati ügykezelő, vagy munkavállaló, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottak, továbbá azon személyek, akik – munkatapasztalat-szerzési, kutatási vagy képzési célból — szakmai gyakorlatukat az ÁEEK valamely szervezeti egységénél végzik.
2. ÁEEK képviselője: adatvédelmi tisztviselő
3. Felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH)

5. A SZABÁLYZAT LEÍRÁSA

5.1. Személyes adatkezelés alapelvei

Az ÁEEK a személyes adatok kezelését a szakmai feladatellátáshoz kötődő, jogszabályban meghatározott feladat- és hatásköreinek, illetve a szervi működést szolgáló – nem szakmai feladatellátáshoz kötődő – belső igazgatási feladatainak (a továbbiakban: funkcionális működéssel kapcsolatos feladatok) ellátása során végzi.

Az ÁEEK a szakmai feladatellátáshoz kötődő feladat- és hatásköreinek ellátása során közérdekű vagy ráruházott közhatalmi jogosítvány gyakorlásával összefüggésben, a feladat végrehajtásához szükséges személyes adatkezelést végez.

Az ügyintézés során csak azokat a személyes vagy különleges adatokat szabad felvenni, amelyek az ügy szempontjából elengedhetetlenül szükségesek. A felvett adatokat csak az adott ügy intézése vagy jogszabályban meghatározott cél érdekében szabad felhasználni, más eljárásokkal, illetve adatokkal nem kapcsolhatók össze.

Az ügyirat részét nem képező, de az eljárás során rögzítésre került személyes és különleges adatokat további felhasználásuk megakadályozása érdekében azonosításra alkalmatlanná kell tenni. az adatkezelési cél megvalósulása után vagy jogalap megszűnésével.

Az A hibás vagy egyéb okból feleslegessé vált adatokat tartalmazó példányokat azonosításra és további felhasználásra alkalmatlanná kell tenni.

Az ügyiratokat az Egységes Iratkezelési szabályzatról szóló főigazgatói utasításnak megfelelően kell kezelni. Az ügyiratok kezelése, tárolása során azok tartalmába az arra feljogosított ügyintézőn kívül más személy – az érintett törvény szerinti betekintési jogán túl – csak akkor tekinthet be, ha ezt a mindenkor hatályos információs önrendelkezési jogról és az információszabadságról szóló törvény szerint hivatali tevékenységével összefüggő feladatellátás szükségessé teszi vagy az érintett kifejezett hozzájárulását.

Az érintett vagy képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ezáltal mások jogai ne sérülhessenek, ennek megfelelően a más személyre vonatkozó személyes adatokat ki kell takarni vagy egyéb módon felismerhetetlenné kell tenni. Ugyanígy szükséges eljárni a másolat, kivonat készítésekor is.

A különleges kategóriába tartozó személyes adat csak a GDPR rendelet 9. cikk (2) bekezdésében megadott valamely feltétel teljesülése esetén kezelhető.

Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot az illetékes főosztály, illetve osztályok vezetőjének, adatgazdának személyre lebontottan meg kell határoznia és az időszerű állapotnak megfelelően nyilván kell tartania.

5.2. Adatbiztonsági szabályok

A jogszabályban meghatározott feladat- és hatáskörök ellátásához kapcsolódó, tartalmuk alapján nem rendszerezett elektronikus vagy papír alapú iratokkal végzett tevékenységek a GDPR rendelet (15) preambulum-bekezdése értelmező bekezdése alapján nem tartoznak a rendelet hatálya alá.

Nem rendszerezett iratnak tekintendő

a) a papír alapú irat, amennyiben az nem valamely adatok nyilvántartására vonatkozó rendszer része, vagy amely kezelése nem nyilvántartási céllal történik;
b) az elektronikus irat, ha kezelő programja nem teszi lehetővé a tartalmára kiterjedő különböző szempontú keresést;
c) az eljárások során készített, nem iktatott papír vagy elektronikus munkaanyag, munkaközi dokumentum, formájától függetlenül (tárolt dokumentum, e-mail).

Az iratok kezelését az ÁEEK a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII.29.) Korm. rendeletnek (a továbbiakban:
335/2005. (XII.29.) Korm. rendelet) megfelelően, az iratkezelési szabályzata alapján végzi.
E tevékenysége során biztosítja, hogy

a) az ügyiratok kezelése, tárolása során azok tartalmába illetéktelen személy betekintést nem nyerhet, az egyes ügyiratokban tárolt személyes adatok védelméért a kijelölt ügyintéző, és az ügyirattal kapcsolatba kerülő más személy felelősséggel tartozik.
b) az iratok tárolása az iratkezelési szabályokban előírtaknak megfelelő ideig történik, a tárolási időt követően az irat jellegétől függően selejtezésre vagy a levéltárnak átadásra kerül.

A munkaközi dokumentumokban, kiadmánytervezetekben rögzített személyes és különleges adatok védelmét az eljárás során és a kiadmányozást követően is biztosítani kell. A nem iktatott papíralapú munkaközi dokumentumokat kiadmányozást követően meg kell semmisíteni, az elektronikus úton előállított munkaközi dokumentumokból a kiadmánytervezeteket és az eljárásra vonatkozó feljegyzéseket, elektronikus leveleket – megőrzés esetén – a megfelelő védettség biztosíthatósága mellett kizárólag az ÁEEK kizárólagos felügyelete alatt álló, illetéktelen hozzáféréstől védett informatikai eszközön lehet tárolni (beleértve az elektronikus iratkezelő rendszert).

Személyes adatokat is tartalmazó elektronikus vagy papíralapú iratot az ÁEEK épületeiből kivinni kizárólag a munkaköri feladat ellátásával összefüggésben, a szervezeti egység vezetőjének engedélyével lehet. A Munkatárs ez esetben is köteles gondoskodni arról, hogy a személyes adatot illetéktelen személy ne ismerhesse meg.

A személyes adatokat is tartalmazó irat és egyéb adathordozó munkaidőn túl csak megfelelő védelmet biztosító helyen (zárható szekrényben) tárolható. A megfelelő tárolás biztosításáért közvetlenül az a felelős, akinél az iratok a munkaidő befejezésekor találhatóak.

Az ÁEEK képviselője a közös használatú nyomtatón vagy másológépen kinyomtatott, illetve lemásolt dokumentumokat haladéktalanul köteles magához venni.

Azokat a helyiségeket, ahol közös használatú nyomtató vagy másológép üzemel, adatbiztonsági követelmények figyelembevételével és betartására tekintettel kell használni.

A Munkatárs köteles a számítógépet és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a számítógépet kikapcsolni, a helyiséget – ahol ez lehetséges – áramtalanítani, az ajtót bezárni és a kulcsot a portaszolgálathoz vagy a szokásos gyűjtő helyre leadni. A személyes adatokat is tartalmazó iratok tárolására szolgáló helyiségeket, valamint az irodahelyiségeket – amennyiben ügyintéző nem tartózkodik ott – munkaidőben is zárni kell.

A személyes adatokat tartalmazó irat a foglalkoztatott általi távoli (beleértve otthoni) elektronikus elérése csak abban az esetben biztosítható, ha az illetéktelenek hozzáférésének kockázata az alkalmazott technikai megoldások miatt alacsony.

Az informatikai úton feldolgozott, tárolt adatok védelmét az ügyintéző jelszavas védelmi rendszere biztosítja. Ezért az adatállományokhoz hozzáférést biztosító jelszó csak az eljárásban, vagy ügyben érintett Munkatársak által és szigorúan bizalmasan kezelendő.

Az ügyintéző a saját belépési jelszavának kizárólagos birtokosa, ez az ő „digitális személyazonossága", senkire át nem ruházható, más Munkatárs vagy harmadik személy számára való felfedése, átadása bármilyen formában szigorúan tilos. Tiltott adattovábbításnak minősül az is, ha a személyes adatok képernyős megjelenítését harmadik személy is megtekintheti.

Az ÁEEK adatvédelmi és adatbiztonsági kockázatai felmérése érdekében a hazai és európai adatvédelmi jogszabályokban rögzítetteknek megfelelően adatvédelmi hatásvizsgálatot folytat le az adatvédelmi tisztviselő bevonásával, amelyet újabb esetleges adatvédelmi /adatbiztonsági kockázatok felmerülése esetében évenként megismétel.

5.3. Iratnyilvántartás

Az ÁEEK a kezelt iratokról a 335/2005. (XII.29.) Korm. rendelet alapján elektronikus nyilvántartást vezet (a továbbiakban: Iratnyilvántartás).

A jogszabály alapján kötelezően vezetett iratnyilvántartás esetében az érintett tiltakozási joga, adatkezelés korlátozásához való joga nem áll fenn.

Az iratnyilvántartás esetében az érintett igényelheti az iratnyilvántartásban tárolt személyes adatai megismerését. Erre vonatkozó kérelmét az ÁEEK iratkezelésért felelős szervezeti egységénél terjesztheti elő, amely az általános ügyintézési határidőn belül azt megválaszolja.

Az iratnyilvántartás esetében az érintett kérelmezheti személyes adatai helyesbítését. Az erre vonatkozó kérelmét az ÁEEK iratkezelésért felelős szervezeti egységénél terjesztheti elő, amely az általános ügyintézési határidőn belül azt megválaszolja. Nem minősül pontatlanul nyilvántartott adatnak a nyilvántartásba vételt követően változott személyes adat, ilyen okból az iratnyilvántartás nem módosítható.

6. A JOGSZABÁLYBAN MEGHATÁROZOTT FELADAT- ÉS HATÁSKÖRÖK ELLÁTÁSÁHOZ KAPCSOLÓDÓ, AZ ÁEEK ÁLTAL NYILVÁNTARTOTT ADATOK KEZELÉSE

6.1. Az adatkezelés jogalapja

A személyes adatok ÁEEK által történő kötelező nyilvántartását igénylő személyes adatkezelést az ÁEEK közvetlen (az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges) jogalap alapján végzi.

6.2. Az adatkezelési feladatok ellátása

Az ÁEEK gondoskodik a GDPR rendelet 24. és 25. és 32. cikkében megszabottak {adatvédelem, adattakarékosság céljából megfelelő technikai és szervezési intézkedések megtétele, adatkezelés biztonsága és annak garantálása) teljesítéséről.

Az érintett fél hozzáférési, helyesbítési jogát – ha jogszabály másképp nem rendelkezik – az ÁEEK-nál gyakorolhatja. Az erre vonatkozó kérelmét a nyilvántartásért felelős szervezeti egységnél vagy az adatvédelmi tisztviselőnél terjesztheti elő, amely az általános ügyintézési határidőn belül azt megválaszolja.

Adatvédelmi tisztviselő központi e-mail címe: **adatvedelmitisztviselo@aeek.hu**

Az ÁEEK által jogszabály alapján vezetett nyilvántartásokban a hozzáférési valamint helyesbítési jog a nyilvántartásra vonatkozó jogszabályban foglaltak szerint – ennek hiányában az általános ügyintézésre vonatkozó szabályok szerint – gyakorolható.

Érintett tiltakozási joggal, illetve korlátozási igénnyel a közvetlen vagy közvetve jogszabályi előírás alapján vezetett nyilvántartások esetében nem élhet.
Az általános tájékoztatási kötelezettség tekintetében az ÁEEK a honlapján tájékoztatást tesz közzé

a) az e fejezet alá tartozó adatkezelések tényéről;
b) az adatvédelmi tisztviselő elérhetőségéről;
c) a személyes adatkezelésben érintettek hozzáférési, helyesbítési jogai gyakorlásához szükséges ügymenetről.

Az e fejezet szerinti, általános közérdeket szolgáló, jogszabályi előírás alapján vezetett nyilvántartásokban történő személyes adat változtatásról más adatkezelők értesítése csak jogszabályban előírtak szerint történhet.

7. FUNKCIONÁLIS MŰKÖDÉSSEL KAPCSOLATOS SZEMÉLYES ADATOK KEZELÉSE

Az ÁEEK a funkcionális feladatainak ellátása során az alábbi feltételek alapján végzi a személyes adatok kezelését

a) az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, vagy
b) az adatkezelés az adatkezelő, az érintett vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, vagy
c) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél.

7.1. Adatkezelői feladatok ellátása

Az ÁEEK a Munkatársakat a felvételt megelőzően vagy a felmerülés időpontjában részletesen tájékoztatja az ÁEEK által végzett rájuk vonatkozó személyes adatkezelésről. A láruházott közhatalmi jogkör gyakorlásához az ÁEEK zavartalan jogszerű működésének biztosíthatósága érdekében az alkalmazás feltétele az adatkezelések tudomásul vétele.

Az érintett Munkatárs részére az ÁEEK – a jogszabályban nem megismerhetőnek előírt adatkörök kivételével – biztosítja a kezelt személyes adataihoz való hozzáférést. A kérelmet a nyilvántartásért felelős szervezeti egységnél kell vagy az adatvédelmi tisztviselőnél kell előterjeszteni.

Az érintett Munkatárs részére az ÁEEK biztosítja a helyesbítési jog gyakorlását. Helyesbítésre vonatkozó kérelmet a téves adat megnevezésével és a helyes adat igazolt megadásával lehet kezdeményezni a nyilvántartásért felelős szervezeti egységnél.

Az ÁEEK a funkcionális működésével összefüggésben vezetett nyilvántartásokból személyes adat átadást csak a jogszabályi előírások szerint teljesít. Ez alól kivételt jelent az adatok technikai adattárolás célú adatfeldolgozása.

Az ÁEEK az alkalmazás megszűnését követően a Munkatársravonatkozó személyes adatokat a jogszabályokban megadott megőrzési ideig tárolja. Ezen adatokra helyesbítés már nem kérhető.

A szerződéses kapcsolatokkal összefüggő adatkezelés esetében az adatokhoz hozzáférés, helyesbítés csak a szerződés egészére vonatkozó hozzáférési, módosítási kérelemként értelmezhető, annak szabályai szerint hajtható végre. Szerződés nyilvántartásával kapcsolatban a tiltakozási jog nem gyakorolható.

Az irat formában történt adatközlésekre vonatkozó adatkezelési nyilvántartás szerepét a funkcionális működést támogató rendszerek mögöttes iktatórendszere tölti be. Az egyéb –közvetlen – formában történő adatkezelések nyilvántartásáról külön gondoskodni kell az adott területnek leginkább megfelelő módon. Megfelelő módnak tekinthető egy alkalmazási program napló adathalmaza, ha a szükséges adatokat tartalmazza, illetve a kézi nyilvántartás is.

Az ÁEEK egyes, a Munkatársakra vonatkozó személyes adat kezelésével kapcsolatos adatkezelésre vonatkozó részletes szabályozást, így különösen

a) a személyügyi adatok kezelésére
b) a bérezéssel kapcsolatos adatok kezelésére
c) nyilvános helyek nagymértékű, módszeres megfigyelésére vonatkozó szabályokat külön szabályzatban adja ki.

8. ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

Az ÁEEK, mint adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységekről írásban - ideértve az elektronikus formátumot is - nyilvántartást vezet. A nyilvántartás tartalmazza a következő információkat:

a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
b) az adatkezelés céljai;
c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR rendelet 49. cikk (1) bekezdésének második bekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
f) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
g) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Az ÁEEK, mint adatfeldolgozó írásban - ideértve az elektronikus formátumot is - nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról.

A nyilvántartás tartalmazza a következő információkat:

a) az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek a nevében az adatfeldolgozó eljár, továbbá - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
b) az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
c) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR rendelet 49. cikk (1) bekezdése második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása.

Az ÁEEK, mint adatkezelő, vagy mint adatfeldolgozó megkeresés alapján a NAIH rendelkezésére bocsátja az általa vezetett adatkezelési tevékenységek nyilvántartását.

9. INFORMATIKAI LEHETŐSÉGEK MAGÁNCÉLRA TÖRTÉNŐ HASZNÁLATÁNAK FELTÉTELEI

A Munkatársak a hivatali elektronikus levelezési (a továbbiakban: e-mail) szolgáltatást hivatali célra vehetik igénybe.

Az ÁEEK nem szankcionálja a magáncélú igénybevételt, de a Munkatársaknak tudomásul kell vennie:

a) a névre szóló hivatali címre érkező bármely e-mail-t informatikai biztonsági okokból az ÁEEK szabályzatban meghatározott felelős munkatársa, a rendszergazda bevonásával elolvashatja,
b) az alkalmazás megszűnését követően az e-mail fiók nem kerül törlésre, mivel a hivatalos célból folytatott kapcsolattartási adatokra az ÁEEK-nak szüksége van.

Az ÁEEK a hivatali munkához nem kapcsolódó elektronikus leveleket a fentieken kívül semmilyen célra nem használja fel, azok illetéktelen megismerés elleni védelmét az alkalmazás megszűnését követően is biztosítja.

Az ÁEEK erre feljogosított Informatikai biztonsági felelőse a biztonsági szempontok érvényesítése érdekében jogosult az elektronikus levelező rendszer adatai megismerésére a GDPR rendelet (49) preambulum-bekezdésben foglaltakkal összhangban. A megismert adat biztonsági szempontokon túl más célra nem használható fel.

Az ÁEEK egyes munkaállomásokon biztosítja a nyilvános internet elérést. Sem munkaidőben, sem azon kívül nem megengedett a munkaállomásokról felkeresni az interneten nem biztonságos, szórakozásra szolgáló, kétes tartalmakat szolgáltató szervereket, zenei vagy film fájlcserélőket, amelyek nem szükségesek a munkavégzéshez. A Munkatárs nyilvános interneten végzett tevékenysége a szervezettől független, otthoni vagy nyilvános helyen végzett tevékenységével azonos megítélés alá esik.

Az internetes kommunikáció során meggondolt, felelős magatartással kell a veszélyforrásokat és valós kockázatokat elkerülni, a védett adatok megszerzésének lehetőségét kizárni. Fentiek be nem tartása, megsértése a Munkatárs fegyelmi és - károkozás esetén - kártérítési felelősségét vonhatja maga után.

Kiemelt jelentősége van a felhasználók részéről az elektronikus információs rendszerekben a vírusbejutás megelőzésének. Ezért tilos idegen vagy kétes eredetű adathordozót helyezni a számítógépbe, továbbá nem nyitható meg azonosítatlan feladótól érkező elektronikus levél melléklete, mert az potenciális vírusveszélyt rejt magában; az ilyen jellegű email-t megnyitás nélkül törölni kell.

A Munkatárs személyes tevékenységével kapcsolatos részletes szabályokat, így különösen az ÁEEK esetében alkalmazott informatikai eszközök és szolgáltatások otthoni használatának szabályait külön szabályzat tartalmazza.

10. SZERVEZETI KÖVETELMÉNYEK

10.1. Betöltendő szerepek

Az ÁEEK a személyes adatok megfelelő védelme érdekében az alábbi feladatköröket nevesíti:

a) adatvédelmi tisztviselő;
b) adatfelelős (szervezeti egység);
c) informatikai biztonsági felelős.

Az adatvédelmi tisztviselő

a) a GDPR rendelet 38. cikk (3) bekezdése alapján feladatai ellátásával kapcsolatban utasítást nem kaphat;
b) közvetlenül a Főigazgatónak tartozik felelősséggel;
c) ellenőrzési jogköre az adatvédelem tekintetében az ÁEEK valamennyi szervezeti egységére kiterjed.

Adatvédelmi tisztviselővé az adatvédelmi jog és gyakorlat szakértői szintű ismeretével rendelkező, Illetőleg az adatvédelemben megfelelő jártassággal bíró személy nevezhető ki.

Az adatvédelmi tisztviselő feladatai:

a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző Munkatársak részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) ellenőrzi az adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is; az ellenőrzés megállapításait ellenőrzési jelentésben rögzíti, amelyet a főigazgató hagy jóvá;
c) tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) az adatkezeléssel összefüggő ügyekben egyeztet a NAIH-hal;
e) vezeti az adatkezelési nyilvántartást;
f) vezeti az adatvédelmi incidensek nyilvántartását.

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

Az adatfelelős az ÁEEK azon önálló szervezeti egysége, amely feladatainak ellátása során személyes adatot kezel. Az adatfelelős működése során kezelt személyes adatokra vonatkozóan gondoskodik az adatvédelmi szabályok megtartásáról.

Az informatikai biztonsági felelős az ÁEEK által kijelölt személy, aki a belső IT rendszerek adatvédelméről, biztonságos üzemeltetéséről, az ÁEEK informatikai ellenőrzési feladatairól gondoskodik.

10.2. Általános felelősségi körök

A jogszabály által védett adatok - ide értve személyes adatokat is - kezelésével kapcsolatos szabályok betartásáról az ÁEEK teljes személyi állománya köteles gondoskodni.

Az adatkezelés és adatfeldolgozási műveletekre vonatkozó –általános érvényű – szabályzatok jogszerűségéért és betartatásáért a főigazgató, az ágazati speciális utasítások betartatásáért a főosztályvezető felel.

Adatfelelős szervezeti egységen belül felmerülő adatvédelmi, adatkezelési, adatfeldolgozási és ügyviteli feladatok tekintetében az illetékes szervezeti egységek vezetői a felelősek.

A Munkatárs, mint adatfeldolgozó tevékenységi körén belül felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, továbbá minden olyan jogsértésért, amit a mindenkor hatályos GDPR rendelet, 2011. évi CXII. törvény: az információs önrendelkezési jogról és az információszabadságról, valamint jelen Szabályzat rendelkezéseinek megszegésével okozott.

11. ADATVÉDELMI INCIDENS KEZELÉSE

11.1. Adatvédelmi incidens bejelentése

A GDPR rendelet 4. cikk 12. pontja szerinti adatvédelmi incidenst az ÁEEK adatvédelmi tisztviselő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A más szerv által vezetett nyilvántartás vagy működtetett szakrendszer esetében, amennyiben az ÁEEK közös adatkezelőnek minősül, az ÁEEK az érintett szervet értesíti, hogy az a szükséges adatokkal kiegészítve – abban az esetben, ha szükségesnek véli – a NAIH értesítését megtehesse.

Az a Munkatárs, aki a személyes adatokkal kapcsolatban adatvédelmi incidenst észlel, így különösen a biztonság olyan sérülését, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi; köteles azt a közvetlen vezetője útján haladéktalanul az adatvédelmi tisztviselőnek bejelenteni.

Amennyiben az adatvédelmi incidens informatikai rendszert érintően következett be, arról haladéktalanul tájékoztatni kell az 1. melléklet megküldésével az informatikai szervezeti egység vezetőjét és az Informatikai biztonsági felelőst.

Az adatvédelmi incidensről szóló bejelentésben az 1. melléklet alapján:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve - ha lehetséges - az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az ÁEEK az adatvédelmi incidensekről nyilvántartást vezet, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

11.2. Az érintett tájékoztatást az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az ÁEEK indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
c) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettet nem kell az adatvédelmi incidensről tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket - mint például a titkosítás alkalmazása -, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

12. ADATKEZELÉSSEL KAPCSOLATOS KÉRELMEK

12.1. A tájékoztatás formája

Az adatkezelésre vonatkozó általános tájékoztató nyilvános, az az ÁEEK honlapján hozzáférhető.

Az ÁEEK a személyes adatok kezelésére vonatkozó tájékoztatását a saját honlapján teszi közzé. Az e módon közzétett tájékoztató a GDPR rendelet 13. cikk (4) bekezdése, illetve 14. cikk (5) a) pontja szerint az érintett által ismertnek tekintendő.

Az érintettet megilleti az a jog, hogy személyes adatai kezeléséről tájékoztatást kérjen. Az adatkezelésre vonatkozó kérelmeket - a jogszabályi feltételek fennállása esetén - legfeljebb 25 napon belül, de lehetőség szerint soron kívül kell teljesíteni. Személyes adatkezelésre vonatkozó egyedi információ csak az érintett személy részére adható.

Az ÁEEK az adatkezelés tárgyát képező személyes adatok elektronikus vagy papír másolatát első kérésekor egy példányban díjfizetés nélkül az érintett rendelkezésére bocsátja.

Az érintett egy hónapon belüli ismételt kérésekor, vagy általa kért további papír másolatokért az adatkezelő az adminisztratív költségeken alapuló díjat számít fel.

Elektronikus kapcsolattartásnál az ÁEEK PDF formátumú dokumentumban küldi meg a válaszát.

Az ÁEEK mindazon adatkezeléseknél, ahol az informatikai háttér a szükséges adatokat tartalmazza, az adatkezelésre vonatkozó tájékoztatást az informatikai rendszerben rögzített adatok alapján teszi meg, külön nyilvántartást nem vezet. Az adatkezelésre, különösen az adattovábbításra vonatkozó nyilvántartásnak minősül:

a) az elektronikus iktató rendszer az irat formában történő adattovábbítás tekintetében
b) az alkalmazási programok napló adatai, az alkalmazás keretében történő adatkezelés tekintetében.

13. SZEMÉLYES ADATNAK NEM MINŐSÜLŐ ADATOK KEZELÉSE

13.1. Védendő adat kezelése

Személyes adatnak nem minősülő, de más okból (különösen üzleti titkot képező) nem nyilvános adat (a továbbiakban: nem nyilvános adat) kezelésére a személyes adat kezelésére vonatkozó szabályokat kell alkalmazni a jelen fejezet szerinti eltérésekkel.

A nem nyilvános adatok kezelésére

a) nem értelmezett a tiltakozási, hozzáférési, korlátozási jog,
b) nem kapcsolódik hozzá tájékoztatási kötelezettség,
c) az adatkezelésről - ha külön jogszabály másként nem rendelkezik - nyilvántartást nem kell vezetni.

A nem nyilvános adatokkal kapcsolatos adatvédelmi incidens esetén

a) hálózaton keresztül bekövetkezett incidens esetén a külön jogszabály szerint a hálózatbiztonsági központ értesítendő,
b) üzleti titkok illetéktelen tudomására jutása esetén az érintettet is értesíteni kell, amennyiben ez lehetséges.

14. ZÁRÓ RENDELKEZÉSEK

Jelen Szabályzat 2018. november 26. napján lép hatályba, ezzel egyidejűleg a 49/2015. főigazgatói utasítás hatályát veszti.

A Szabályzat felülvizsgálatáért és módosításáért – évenkénti rendszerességgel – az adatvédelmi tisztviselő felelős.