MAGYAR ORVOSI KAMARA

FOGORVOSOK TERÜLETI SZERVEZETE

Adatkezelési és Adatvédelmi Szabályzat

2024. év

Adatvédelmi és adatbiztonsági szabályzat

Általános rendelkezések

Szabályzat célja

1. Az Adatvédelmi és adatbiztonsági szabályzat (továbbiakban: Szabályzat) célja annak biztosítása, hogy a **Magyar Orvosi Kamara Fogorvosok Területi Szervezete** (székhely: 1068 Budapest, Szondi u. 100., adószám: 19637877-2-42) (továbbiakban: Adatkezelő) megfeleljen 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, az Európai Parlament és a Tanács 2016/679 Rendeletében (a továbbiakban: GDPR rendelet), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (továbbiakban: Infotv.) foglaltaknak.

2. A Szabályzat célja az Adatkezelő által adatkezelői, illetve adatfeldolgozói minőségben kezelt és feldolgozott személyes adatok védelmi rendszerének kiépítése és működtetése.

3. Az Adatkezelő által kezelt és feldolgozott személyes adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, véletlen megsemmisülés és sérülés, valamint az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Szabályzat hatálya

4. A Szabályzat személyi hatálya kiterjed az Adatkezelő valamennyi munkatársára, vele bármilyen szerződés jogviszonyban állókra.

5. A kötendő szerződésekben biztosítani kell a Szabályzat rendelkezéseinek érvényesülését az Adatkezelővel, mint megrendelővel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és egyéb szervezetek, valamint ezek alkalmazottai (továbbiakban: külső támogatók) vonatkozásában, továbbá biztosítani kell, hogy az érintett személyek a Szabályzatot (eseti kivonatát) a szükséges mértékben megismerjék.

6. Az Adatkezelővel, mint szolgáltatóval kötött szerződések esetében a Szabályzatban foglaltakat a szerződés előkészítésekor irányadónak kell tekinteni.

7. A Szabályzat tárgyi hatálya kiterjed az Adatkezelő bármely — személyes adatot érintő — számítógépes és manuális adatkezelésre, adatfeldolgozásra.

Hivatkozások

8. A Szabályzatot a jogszabályokkal összhangban kell alkalmazni, különösen, de nem kizárólagosan a következőkkel:

a) Magyarország Alaptörvénye,
b) 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, az Európai Parlament és a Tanács 2016/679 Rendelete (GDPR rendelet),
c) 2016. évi CXXX. törvény a polgári perrendtartásról (Pp.),
d) 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.),
e) 2012. évi l. törvény a Munka Törvénykönyvéről (Mt.),
f) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.),
g) 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Vvtv.),
h) 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről,
i) 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról, és a magánlevéltári anyagok védelméről (Ltv.),
j) 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről.

9. A Szabályzatot az alábbi belső szabályozó eszközökkel összhangban kell alkalmazni:

Adatvédelmi politika

Fogalom meghatározások

10. A Szabályzat alkalmazása során az alábbiakban részletezett fogalmak irányadók.

Fogalom	Definíció
adatfeldolgozó	GDPR rendelet 4. cikk 8. pont alapján: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
adathordozó	Olyan eszköz, amely alkalmas adatok megőrzésére, tárolására. Megjelenési formája szerint lehet: papíralapú, vagy elektronikus.
adatkezelés	GDPR rendelet 4. cikk 2. pont alapján: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyújtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.
adatkezelő	GDPR rendelet 4. cikk 7. pont alapján: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.
adatvédelmi incidens	GDPR rendelet 4. cikk 12. pont alapján: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
biztonsági esemény	IBSZ alapján: lbtv. 1. S 9. pont alapján: biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
biztonságtechnikai rendszerek	Távfelügyeleti átjelzéssel vagy anélkül üzemeltetett behatolásjelző, beléptető, kamera- és tűzjelző rendszer.

Elektronikus információs rendszer	Ibtv]l. S (1) bekezdés 14b. pontja alapján: a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.
érintett	GDPR rendelet 4. cikk 1. pont alapján: azonosított vagy azonosítható természetes személy.
harmadik fél	GDPR 4. cikk 10. pont alapján: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
hozzájárulás	GDPR 4. cikk 11. pont alapján: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
információs önrendelkezési jog	Alaptörvény VI. cikk alapján: a személyes adatok védelmét garantáló állampolgári alapjog, tárgya a személyes adat.
a személyes adatok különleges kategóriái	GDPR rendelet 9. cikk (1) bekezdés alapján: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
személy- és munkaügyi nyilvántartás	A HR által vezetett, a munkavállaló — munkaviszonnyal összefüggésben keletkezett és azzal kapcsolatban álló — adatait tartalmazó nyilvántartás.
személyes adat	GDPR rendelet 4. cikk 1. pont alapján: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Rövidítések

11. A Szabályzatban az alábbi rövidítések fordulnak elő.

Rövidítés	Definíció
HR	Humánerőforrás
IT	Informatika

Adatvédelmi alapelvek

12. Az Adatkezelő által végzett adatkezelések, adatfeldolgozások során az alábbi adatvédelmi alapelveknek kell érvényesülniük.

Jogszerűség, tisztességes eljárás és átláthatóság

13. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Az adatkezelés akkor jogszerű, ha megfelelő jogalappal bír. Akkor átlátható és tisztességes, ha az adatkezelő és az adatkezelés célja világosan meghatározott, az érintett az adatkezelésről és jogai gyakorlásának módjáról megfelelő tájékoztatást kapott. A tájékoztatásnak könnyen hozzáférhetőnek és közérthetőnek kell lennie.

A célhoz kötöttség elve

14. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a statisztikai célból történő további adatkezelés. Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája, hogy az adatkezelés csak pontosan meghatározott és jogszerű célból történhet.

Az adattakarékosság elve

15. A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük és a szükségesre kell korlátozódniuk. Az adattakarékosság elvének teljesülése adatkezelésenként mérlegelendő, és új adatkezelés esetén már az adatkezelés folyamatának megtervezésekor figyelembe kell venni.

A pontosság elve

16. A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

A korlátozott tárolhatóság elve

17. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak jogszabály általi kötelezés vagy pl. statisztikai célból kerülhet sor. Amennyiben tehát az adatkezelési cél teljesült, az adatokat törölni vagy anonimizálni kell. Az adatkezelőnek rendszeres időközönként vizsgálnia kell, hogy a megőrzési idő letelt-e.

Integritás és bizalmas jelleg

18. A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Elszámoltathatóság

19. Az adatkezelő felelős az adatkezelési elveknek való megfelelésért, továbbá képesnek kell lennie a megfelelés igazolására.

Az érintettek jogai és érvényesítésük

Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

20. Az Adatkezelő az érintettet az adatkezelést megelőzően tájékoztatja. A tájékoztatás megtörténhet úgy is, hogy az adatkezelés részleteiről szóló tájékoztatót az Adatkezelő közzéteszi és erre az érintett figyelmét felhívja.

21. Az érintett kérelmére az Adatkezelő tájékoztatást ad az Adatkezelő kilétéről és elérhetőségéről, az adatvédelmi tisztviselő elérhetőségéről, az érintett általa kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről, az adatkezeléssel összefüggő tevékenységéről, az érintett személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről, továbbá az érintett által gyakorolható jogokról, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) címzett panasz benyújtásának jogáról.

22. Az Adatkezelő elősegíti az érintett jogainak a gyakorlását. Az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb időn belül, legfeljebb azonban egy hónapon belül közérthető formában a tájékoztatást megadni. A tájékoztatás csak akkor tagadható meg, ha az Adatkezelő bizonyítja, hogy az érintettet nem áll módjában azonosítani. Amennyiben az Adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a NAIH-nál és élhet bírósági jogorvoslati jogával.

Az érintettnek szóló tájékoztatást díjmentesen biztosítja az Adatkezelő. Ha az érintett kérelme egyértelműen megalapozatlan vagy — különösen ismétlődő jellege miatt — túlzó, az Adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre ésszerű összegű díjat számíthat fel vagy

23. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az Adatkezelőt terheli.

24. Az érintett kérdéseire az Adatkezelő egy hónapon belül válaszol.

Hozzáféréshez való jog

25. Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arról, hogy adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy az alábbi információkhoz hozzáférést kapjon:

a) adatkezelés célja,
b) érintett személyes adatok kategóriái,
c) adatok címzettjei,
d) adattárolás időtartama,
e) érintetti jogok,
f) jogorvoslat,
g) adatok forrása, ha nem az érintettől gyűjtötték őket.

26. Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérelmére rendelkezésére bocsátja. Amennyiben az érintett elektronikus úton nyújtotta be a kérelmet, az információkat elektronikus formátumban kell rendelkezésére bocsátani, kivéve, ha az érintett másként kéri.

A helyesbítéshez való jog

27. Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

A törléshez való jog

28. Az Adatkezelő az érintett kérésére köteles törölni az érintettre vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:

a) az adatkezelés már nem szükséges,

b) az érintett visszavonja a hozzájárulását és az adatkezelésnek nincs más jogalapja,
c) az érintett tiltakozik az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
d) a személyes adatokat jogellenesen kezelték.

29. A törlés nem alkalmazható, ha az adatkezelés jogi kötelezettség teljesítése érdekében történik (pl. a megőrzési időt jogszabály írja elő) vagy jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez szükséges.

Adatkezelés korlátozásához való jog

30. Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha

a) az érintett vitatja a személyes adatok pontosságát (az ellenőrzéshez szükséges ideig),
b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését,
c) az Adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat,
d) az érintett tiltakozott az adatkezelés ellen (amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben).

31. A korlátozást az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani (ideiglenes áthelyezés másik adatkezelő rendszerbe, és vagy megjelölés). Az adatokon a tárolás kivételével további adatkezelési műveletek nem végezhetők, az adatokat nem lehet megváltoztatni. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.

Adathordozhatósághoz való jog

32. Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha

a) az adatkezelés hozzájáruláson vagy szerződésen alapul és
b) az adatkezelés automatizált módon történik.

Tiltakozáshoz való jog

33. Az érintett jogosult arra, hogy bármikor tiltakozzon személyes adatainak kezelése ellen az alábbi esetekben:

a) az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges,
b) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,
c) az adatkezelés tudományos és történelmi kutatási célból vagy statisztikai célból történik.

34. A tiltakozáshoz való jogra az érintett figyelmét legkésőbb az első kapcsolatfelvétel során fel kell hívni, és az erre vonatkozó tájékoztatást elkülönítve kell megjeleníteni.

Az érintetti jogok teljesítésének eljárásrendje

35. Az érintett a tájékoztatás, hozzáférés, helyesbítés, korlátozás vagy törlés, továbbá az adathordozás iránti kérelmét és tiltakozását az Adatkezelőhöz, vagy az adatvédelmi tisztviselőhöz nyújthatja be.

36. Az adatkezeléssel kapcsolatos tájékoztatási és intézkedési igényről az adatvédelmi tisztviselőt értesíteni kell.

37. Az érintettnek való megküldés előtt a tájékoztatást, intézkedést tartalmazó levelet meg kell küldeni az adatvédelmi tisztviselőnek olyan időben, hogy a nyitva álló legfeljebb egy hónapból még legalább 15 munkanap rendelkezésre álljon. Az adatvédelmi tisztviselő megvizsgálja a levéltervezetben foglaltakat, amennyiben nem az adatvédelmi tisztviselő volt a kérelem címzettje — visszaküldi a tájékoztatást, intézkedést tartalmazó levelet, az Adatkezelőnek, aki megküld meg az érintettnek.

38. Helyesbítés, korlátozás, törlés, illetve adathordozás és tiltakozás iránti kérelem esetén is egyeztetni szükséges az adatvédelmi tisztviselővel a kérelem teljesíthetőségéről, illetve annak módjáról. Ha az Adatkezelő az érintett kérelmét nem teljesíti, úgy egy hónapon belül közli az elutasítás okát és tájékoztatja az érintettet a jogorvoslati lehetőségekről.

39. A jogellenes adatkezeléssel okozott kárért az Adatkezelő a vonatkozó jogszabályokban meghatározott szabályok szerint felel. Az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével okozott kárt köteles megtéríteni. Az érintettel szemben az Adatkezelő felel az adatfeldolgozó által okozott kárért is. Az Adatkezelő általános polgári jogi felelősségére a Ptk. vonatkozó rendelkezései az irányadók.

Az Adatkezelő adatvédelmi intézményrendszere

40. Az adatvédelmi előírások alkalmazása során a szerv vezetőjének az Adatkezelő elnöke minősül.

41. Az Adatkezelő vezetője határozatlan időre az adatvédelmi jogot és gyakorlatot szakértői szinten ismerő adatvédelmi tisztviselőt nevez ki.

42. Az adatvédelmi tisztviselő

a) tájékoztat és szakmai tanácsot ad az Adatkezelő, továbbá a munkatársak részére a GDPR rendelet, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) ellenőrzi a GDPR rendeletnek, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezéseknek, továbbá az Adatkezelő személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) együttműködik a Hatósággal és
e) az adatkezeléssel összefüggő ügyekben — ideértve a GDPR rendelet 36. cikkében említett előzetes konzultációt is — kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

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

44. Az adatvédelmi tisztviselőhöz bármely érintett fordulhat.

45. Az Adatkezelő az adatvédelmi tisztviselő elektronikus és postai elérhetőségét közzéteszi az Adatkezelő honlapján, az adatkezelési tájékoztatóban az alábbiak szerint:

46. Az Adatkezelő adatvédelmi tisztviselője: név: dr. László Tünde Hilda, e-mail cím: drlaszlotunde@t-online.hu,

A munkatársak, álláskeresők személyes adatainak kezelése

Az Adatkezelő toborzási, kiválasztási tevékenységével kapcsolatos adatkezelés

47. Az Adatkezelő lehetővé teszi az álláskeresők számára, hogy önéletrajzuk és motivációs levelük megküldésével jelentkezzenek az Adatkezelőnél meghirdetett, betöltetlen álláshelyekre. A szükséges személyes adatok körét, az adatkezelés jogalapját, célját és időtartamát az ebből a célból létrehozott Adatkezelési tájékoztató toborzási és kiválasztási tevékenységhez című dokumentum tartalmazza.

48. Az Adatkezelő a különböző módokon beérkező pályázatokat egységesen a kiválasztási eljárás lezárultát követő 6 hónapig őrzi meg.

A munkatársak személyes adatainak kezelése

49. Az Adatkezelő a munkatársainak személyes adatait a munkaviszony, munkavégzésre irányuló egyéb jogviszony létesítésével, fennállásával és megszüntetésével, valamint az abból származó jogok gyakorlásával és kötelezettségek teljesítésével összefüggésben kezelheti.

50. A személyügyi nyilvántartás vezetéséhez az érintett munkatárs saját magára vonatkozóan köteles adatot szolgáltatni. A nyilvántartás adatkörében beállt változásról az érintett köteles azonnali hatállyal írásban bejelentést tenni.

51. Törvényi felhatalmazás hiányában az adatkezelés alapjául kizárólag a munkaviszonyt, munkavégzésre irányuló egyéb jogviszonyt létrehozó szerződés teljesítése vagy Az Adatkezelő jogos érdeke, illetve kivételes esetben a munkatárs számára egyértelműen kedvező, csak előnnyel járó esetekben a munkatárs, illetve új belépő munkatárs előzetes, megfelelő tájékoztatáson alapuló, önkéntes és határozott hozzájárulása szolgálhat, amelyben félreérthetetlen hozzájárulását adja a rá vonatkozó személyes adatok meghatározott célból és körben történő kezeléséhez.

52. A munkatárstól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely a személyhez fűződő jogát nem sérti és a munkaviszony létesítése, teljesítése vagy megszüntetése szempontjából szükséges.

53. A munkatársat tájékoztatni kell arról, hogy

a) milyen adatait, milyen célból és jogalappal, mennyi ideig kívánja az Adatkezelő kezelni,
b) az adatok továbbítására milyen célból és mely szervek részére kerülhet sor,
c) az adatkezeléssel kapcsolatban milyen jogokkal rendelkezik (hozzáférés, helyesbítés, korlátozás, törlés kezdeményezése, adathordozás, tiltakozás),
d) milyen jogorvoslati lehetőséggel rendelkezik.

54. Az Adatkezelő a munkatársra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy az 53. pontban felsorolt jogalapok valamelyikének fennállása esetén közölhet. Törvényben meghatározott esetnek minősül a munkavállalói adatok közlése az adóhatóság és a társadalombiztosítási, munkaerő-piaci szervek felé is.

55. Az Adatkezelő a munkatársat a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. Az Adatkezelő ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkatárs magánélete — különös tekintettel a személyes adatok különleges kategóriáiba tartozó adatokra — nem ellenőrizhető, kivéve a külön jogszabály által szabályozott, nemzetbiztonsági ellenőrzés, illetve a hatósági erkölcsi bizonyítvány bekérése esetén.

56. Az Adatkezelő előzetesen tájékoztatja a munkatársat azokról az eljárásokról, valamint technikai eszközöknek az alkalmazásáról, amelyek a munkatárs ellenőrzésére szolgálnak.

57. Új belépő munkatársat a fentiekről az Adatkezelő tájékoztatja a beléptetési folyamat során, valamint a helyben szokásos módon.

58. Az Adatkezelő köteles biztosítani, hogy a munkatárs a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról — titoktartási nyilatkozat megtételével — másolatot vagy kivonatot kaphasson.

59. A munkatárs

a) kérheti adatai helyesbítését, illetve kijavítását,
b) kérheti adatainak törlését a jogszabályi rendelkezésekben foglalt korlátozásokkal,
c) jogosult megismerni, hogy a személy- és munkaügyi nyilvántartásban kezelt adatait kinek, milyen célból és milyen adatkört érintően továbbították.

60. Az Adatkezelő korlátozza az adatkezelést, ha a munkatárs ezt kéri és a jogszabályban felsorolt esetek valamelyike fennáll. Korlátozás esetén az érintett adatokon a tárolás kivételével további adatkezelési műveletek nem végezhetők, az adatokat nem lehet megváltoztatni. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell. A korlátozás alá eső személyes adatokat kezelni lehet, ha az érintett hozzájárul, méltányolható magánérdek védelme érdekében, más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve az állam fontos közérdekéből.

61. A munkatárs bizonyos munkakörök betöltése esetén hatósági erkölcsi bizonyítványával köteles igazolni, hogy nem szerepel Magyarország bűnügyi nyilvántartásában.

62. A személy- és munkaügyi nyilvántartás jogszerűségéért, a személyes adatok védelméért az Adatkezelő vezetője felelős.

63. A munkatárs személyi iratai körébe az alábbiak tartoznak:

a) személyi anyag: az Mt. szerint kért vagy a munkavégzésre irányuló jogviszonyhoz szükséges és keletkezett iratok, a személyi adatlap, önéletrajz, a munkatárs felvételére vonatkozó javaslat, a

munkaszerződés és annak módosítása, munkaviszonyt megszüntető irat, írásbeli figyelmeztetésre, kártérítési felelősség megállapítására vonatkozó irat,

b) a munkatárs munkaviszonyával összefüggő egyéb irat,
c) a munkatárs kérelmére kiállított vagy önként átadott adatokat tartalmazó irat.

64. A személyi iratokba jogosult betekinteni:

a) a munkatárs a saját adataiba,
b) a munkatárs felettese,
c) a munkatárs kötelezettségszegése miatt indult eljárás során az azt lefolytató testület vagy személy,
d) munkaügyi per kapcsán a bíróság,
e) a munkaviszonnyal összefüggésben indult büntetőeljárásban a nyomozó hatóság, az ügyész és a bíróság,
f) a személyes adatok kezelésével összefüggésben végzett vizsgálata során a NAIH,
g) a személyügyi, munkaügyi és bérszámfejtői, valamint a képzési, toborzási, kiválasztási feladatokat ellátó szervezet vagy személy.

65. A munkatársak személyi iratainak kezelése során a személyi iratnak csak a — néven kívül egyéb személyes adatot nem tartalmazó — fedőlapja továbbítható, a felelős személyek megjelölésekor a személyes adatok védelme érdekében különös figyelemmel kell lenni arra, hogy az adott személyes adatot csak az arra jogosult ismerhesse meg,

66. Az Adatkezelő által kötött szerződések esetében a szerződés teljesítéséhez szükséges adatkezelés mint jogalap alapján az Adatkezelővel szerződő fél a szükséges mértékben és ideig, legfeljebb azonban a szerződésből származó jogok érvényesíthetőségének elévüléséig jogosult Az Adatkezelő nevében és megbízásából eljáró munkatársak szerződésben feltüntetett alábbi személyes adatait kezelni:

a) munkatárs neve,
b) munkahelyi e-mail címe,
c) munkahelyi telefonszáma.

A munkahelyi számítógép, az e-mail és az internet, valamint a munkahelyi telefon használatának ellenőrzése

Az Adatkezelő a számítógép, az e-mail és az internet, valamint a mobiltelefon használatának rendjéről külön szabályzatot alkothat.

67. Az adatkezelés célja a munkaviszonyból származó kötelezettségek teljesítésének ellenőrzése, elszámolás, jogalapja az Mt. 11/A. §-a, valamint a GDPR rendelet (49) preambulum bekezdése szerinti jogos érdek.

68. A munkatársak az Adatkezelő által munkavégzés céljából rendelkezésükre bocsátott infokommunikációs eszközöket (pl. számítógép, mobiltelefon) kizárólag munkavégzésre használhatják, melynek megvalósulását az Adatkezelő ellenőrizheti. Az ellenőrzés során az Adatkezelő a munkaviszonnyal összefüggő, a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt adatokba tekinthet be addig, ameddig nem tudja eldönteni, hogy az adat magáncélú adat-e.

69. Az Adatkezelő által biztosított e-mail címhez tartozó postafiók esetében az Adatkezelő vezetője által kijelölt személy jogosult ellenőrizni, hogy annak használata csak munkavégzéssel összefüggően történt-e, azzal a feltétellel, hogy a magánjellegű levelek tartalma nem ismerhető meg.

70. Az a tény, hogy ki milyen online tartalmakat, internet oldalakat és milyen gyakorisággal tekint meg, személyes adatnak minősül. Mivel az Adatkezelő a munkahelyi internethasználatot munkavégzés céljából teszi lehetővé, illetve a magánhasználatot korlátozza, az Adatkezelő jogosult annak ellenőrzésére, hogy azt a munkatárs a munkaviszonyával összhangban használja-e. Az Adatkezelő nem vizsgálhatja az internethasználatból következő, abból kideríthető magán jellegű információkat. Az ellenőrzésnek annak megállapítására kell korlátozódnia, hogy az internethasználat megfelelő mértékben szolgálja-e a munkatárs munkaköri feladatainak ellátását, szakmai tájékozottságának növelését, illetve nem valósít-e meg az Adatkezelő által tilosként deklarált tevékenységet. Az ellenőrzés során a munkatárs Indoklását is figyelembe kell venni az olyan esetekben, amikor objektív szempontok alapján nem egyértelmű, hogy az internethasználat megfelel-e az Adatkezelő elvárásainak, szabályainak.

71. A 71-72. pont szerinti ellenőrzésről értesíteni kell a munkatársat, lehetőséget biztosítva arra, hogy az ellenőrzésen a munkavállaló részt vegyen és az ellenőrzés megállapításaival kapcsolatosan írásban észrevételt tegyen. Amennyiben az informatikai biztonság érdekében megteendő intézkedés sürgőssége indokolja, a munkatárs értesítése utólag is megtörténhet. A munkatárs ez esetben is megteheti észrevételeit.

72. Biztonsági esemény megelőzése, illetve észlelése esetén az Adatkezelő annak vizsgálata céljából jogosult az elektronikus információs rendszerben tárolt adatokhoz való hozzáférésre, az adatok észlelésére. Az adatkezelés jogalapja a GDPR rendelet (49) preambulum bekezdése szerinti jogos érdek. Az Adatkezelő ilyen esetben akkor jogosult az adott személyes adat megismerésére, ha megalapozottan feltételezhető, hogy az adott adatot tartalmazó fájl, dokumentum stb. az okozója a biztonsági esemény közvetlen veszélyének vagy megtörténtének. A személyes adat megismeréséről az érintett munkatársat tájékoztatni kell, bemutatva a megismerés okait.

Az Adatkezelő munkatársai által alkalmazandó általános adatkezelési szabályok

73. Az Adatkezelő valamennyi munkatársa köteles a személyes adatok kezelése vonatkozásában az alábbi gyakorlati szabályokat megtartani:

a) A munkavégzés során csak az ahhoz elengedhetetlenül szükséges személyes adatok kezelhetők, továbbíthatók, az Adatkezelő vezetőjének felelőssége a munkafolyamatok ennek megfelelő kialakítása (szükségtelen adathalmozás elkerülése).
b) Az informatikai jogosultságok engedélyezésekor figyelemmel kell lenni arra, hogy személyes adathoz csak az férhessen hozzá, akinek a munkavégzéséhez az az adat, adatkör elengedhetetlenül szükséges (érvényesüljön a legkisebb jogosultság elve). Informatikai rendszerhez való hozzáférési jogosultságot, a „Belső informatikai rendszerhez való hozzáférési jogosultság” (1. számú melléklet) nyomtatvány használatával adható meg.
c) E-mailben személyes adatot tartalmazó dokumentum csak úgy továbbítható, hogy biztosított legyen, hogy azt csak az arra jogosult tekintheti meg. A kiküldendő levelet a kiküldést megelőzően ellenőrizni kell, hogy a megfelelő e-mail címek szerepelnek-e a címzettek között (az illetéktelen megismerést elkerülendő), illetve azt is mérlegelni kell, hogy az e-mail címeket nem indokolt-e rejtett módon rögzíteni a „titkos másolat” funkcióval. A levélváltási előzményeket is vizsgálni szükséges, hogy tartalmaz-e védendő személyes adatot; indokolt esetben gondoskodni kell az előzmények törléséről vagy elhagyásáról.
d) A közösen használt meghajtókon személyes adatot tartalmazó dokumentum csak akkor tárolható, ha biztosított, hogy azt csak az arra jogosultak tekintik meg.
e) Az adatvédelmi tisztviselőnek lehetőség szerint gondoskodnia kell a munkatársak megfelelő adatvédelmi és adatbiztonsági képzéséről, továbbképzéséről.

Az Adatkezelő, mint adatfeldolgozó

74. Ha az Adatkezelő, mint adatfeldolgozó jár el, tevékenysége során az alábbi előírások érvényesülnek:

a) az adatfeldolgozó az adatkezelő által meghatározott adatkezelési műveleteket végzi, és e minőségében gyakorolja az adatkezelő által ráruházott jogosultságokat, teljesíti kötelezettségeit,
b) al-adatfeldolgozó igénybevétele esetén az adatkezelés céljának és idejének, a kezelt adatok körének meghatározására, az adatkezelésre vonatkozó érdemi döntések meghozatalára továbbra is az adatkezelő jogosult és köteles, az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel,
c) az Adatkezelő adatfeldolgozóként az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, a személyes adatokat az adatkezelő rendelkezéseinek és a jogszabályi előírásoknak megfelelően köteles tárolni és megőrizni,
d) az adatfeldolgozásra vonatkozó szerződést írásban kell megkötni, a GDPR rendelet 28. cikkének (3) bekezdésében felsorolt tartalmi elemekkel,
e) az Adatkezelő az adatfeldolgozó tevékenységi körén belül, illetve az adatkezelő által meghatározott keretek között felelős a személyes adatok kezeléséért,

f) az Adatkezelő, mint adatfeldolgozó az adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót,
g) az Adatkezelő, mint adatfeldolgozó a feldolgozással érintett személyes adatokat harmadik személy vagy szerv részére az adatkezelő előzetes, dokumentált hozzájárulása nélkül nem továbbíthatja. Kivételt képez, amikor az adatfeldolgozót jogszabály kötelezi arra, hogy az adatokat továbbítsa az adatkérő hatóság, bíróság felé.

Adatbiztonság, adatvédelmi incidens

75. Az Adatkezelő gondoskodik az adatok biztonságáról. Ennek érdekében a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megteszi a szükséges technikai és szervezési intézkedéseket, amelyek az irányadó jogszabályok, adat és titokvédelmi előírások érvényre juttatásához szükségesek mind az elektronikus információs rendszerben tárolt, mind a hagyományos, papír alapú adathordozókon tárolt adatállományok tekintetében.

76. Az Adatkezelő az adatokat — az alkalmazott eljárásokkal és technikai eszközökkel — védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

77. Az Adatkezelő fenntartja azt a jogot, hogy az adatbiztonság szabályainak érvényesítése céljából a munkatársak személyes adataiba és az Adatkezelő által kezelt egyéb személyes adatokba betekintést nyerjen. Az adatkezelés jogalapja ezekben az esetekben a GDPR rendelet (49) preambulum bekezdése szerinti jogos érdek. E betekintési jogot Az Adatkezelő nevében Az Adatkezelő vezetője, az elektronikus információs rendszerben tárolt adatok esetén, a 84. pontban szabályozott biztonsági eseménnyel kapcsolatban általa kijelölt személyek gyakorolják.

78. Az Adatkezelő az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. Az Adatkezelő a több lehetséges adatvédelmi és adatbiztonsági megoldás közül azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

79. Az Adatkezelő az elektronikus információs rendszerben tárolt adatok védelme körében gondoskodik különösen:
a) az adminisztratív és a logikai védelmi intézkedésekről, beleértve a jogosulatlan hozzáférés elleni védelmet is,
b) az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről,
c) az adatállományok kártékony kódok elleni védelméről,
d) az adatállományok, illetve az adatokat hordozó eszközök fizikai védelméről, ezen belül az objektumvédelmi intézkedések megtételéről, valamint a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról.

80. A munkatársak és az Adatkezelő 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.

81. Adatvédelmi incidens bekövetkezése esetén haladéktalanul értesíteni kell az adatvédelmi tisztviselőt, valamint az incidens jellegétől függően rendszergazdát, részletesen ismertetve az incidens valamennyi ismert részletét és az adatvédelmi incidens elhárítása érdekében esetlegesen már megtett intézkedéseket. Az adatvédelmi tisztviselő és az incidenst bejelentő, az Adatkezelő vezetői mérlegelik, hogy az incidens kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve. Amennyiben igen, az adatvédelmi tisztviselő az adatvédelmi incidens tudomásra jutásától számított 72 órán belül az incidenst bejelenti a NAIH-nak.

82. Amennyiben az Adatkezelő az incidenssel érintett adatkezelés tekintetében adatfeldolgozóként jár el, az incidensről való tudomásszerzését követően indokolatlan késedelem nélkül jelzi azt az adatkezelőnek.

83. A NAIH-nak való bejelentésben legalább

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 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.

84. Amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

85. Az adatvédelmi tisztviselő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

86. Jelen szabályzat 2. számú melléklete az adatvédelmi incidensek kezelésére szolgáló Adatvédelmi incidenskezelési terv.

Adattovábbítás

87. Adatok továbbítására minden esetben csak jogszerű jogalap fennállása esetén kerülhet sor.

88. A jogszabályon alapuló, és az eseti adatszolgáltatás esetén minden esetben meg kell győződni az adatkezelés jogalapjáról, kétség esetén az adatvédelmi tisztviselő közreműködését kell kérni. Személyes adatot továbbítani csak abban az esetben lehet, ha annak jogalapja egyértelmű, célja és az adattovábbítás címzettjének a személye pontosan meghatározott. Az adattovábbítást minden esetben dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen.

89. A jogszabály által előírt adattovábbítást az Adatkezelő köteles teljesíteni.

90. Amennyiben az adattovábbításhoz az érintett hozzájárulására van szükség, a hozzájárulás megtörténtét dokumentálni kell. Az érintettek hozzájárulásához kötött adattovábbítás esetén az érintett írásbeli nyilatkozatát az adattovábbítás címzettje és célja ismeretében adja meg.

A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása

91. A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítására kizárólag a GDPR rendelet V. fejezetében megállapított esetekben és garanciák mellett kerülhet sor.

Ellenőrzés

92. Az adatvédelemmel kapcsolatos jogszabályi előírások és belső szabályozó eszközök előírásainak megtartását az adatkezelést végzők kötelesek folyamatosan ellenőrizni a Szabályzat alapján.

93. Az adatvédelmi tisztviselő jogosult az adatvédelemmel kapcsolatos általános és célellenőrzéseket végezni. Az adatbiztonsággal összefüggő ellenőrzések során az adatvédelmi tisztviselővel a munkatársak kötelesek együttműködni.

94. Az ellenőrzésre feljogosított személy 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.

95. Az adatvédelmi tisztviselő jogosult az irat- és adatkezeléssel kapcsolatos belső szabályozó eszközök, dokumentumok, jegyzőkönyvek és nyilvántartások áttekintésével ellenőrizni az adatkezelés rendjének megtartását. Jogszabálysértés esetén annak megszüntetésére szólítja fel az adatkezelő személyt, különösen súlyos jogszabálysértés esetén pedig az Adatkezelő igazgatójához fordul. Az adatvédelmi tisztviselő jogosult a személy- és munkaügyi nyilvántartások rendszerét ellenőrizni.

Az adatvédelmi rendelkezések megsértése esetén követendő eljárás

96. Amennyiben valamely személynek tudomására jut, hogy a vonatkozó jogszabályokban vagy a Szabályzatban foglalt adatvédelmi és adatbiztonsági rendelkezéseket megsértették, illetve ennek veszélye áll fenn, Az Adatkezelő igazgatóját vagy az adatvédelmi tisztviselőt.

97. Az Adatkezelő igazgatója az adatvédelmi tisztviselő bevonásával haladéktalanul intézkedik:

a) a személyes adatok védelmi rendszerének helyreállításáról,
b) a rendelkezések megsértésére vezető okok, illetve az azt elősegítő körülmények feltárásáról,
c) az érintett személy(ek) felelősségének tisztázásáról,

NAIH vizsgálatában való közreműködés

98. A NAIH jogosult az Adatkezelőnél ellenőrizni az adatvédelmi szabályok megtartását, illetve kivizsgálni a hozzá érkező panaszokban foglaltakat.

99. A NAIH-nál panasz benyújtásával bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy a személyes adatok kezelésével kapcsolatban az Adatkezelőnél jogsérelem következett be vagy annak közvetlen veszélye áll fenn.

100. Az Adatkezelő a NAIH-hal együttműködik, a NAIH kérésének a NAIH által megállapított határidőn belül eleget tesz, illetve amennyiben a NAIH által tett megállapításokkal, illetve a NAIH által meghatározott határozatokkal nem ért egyet, megteszi a GDPR rendeletben meghatározott lépéseket.

101. A vizsgálatban meghatározott feladatok teljesítését az adatvédelmi tisztviselő koordinálja.

Az adatkezelési tevékenységek nyilvántartása

102. Az Adatkezelő az általa végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:

a) az adatkezelés céljai,
b) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése,
c) adott esetben az olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket,
d) 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 albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása,
e) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők,
f) ha lehetséges, az adatbiztonság érdekében megtett technikai és szervezési intézkedések általános leírása.

103. Az Adatkezelő, mint adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

a) minden olyan adatkezelő neve, amelynek vagy akinek a nevében az adatfeldolgozó eljár,
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) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása,
d) ha lehetséges, az adatbiztonság érdekében megtett technikai és szervezési intézkedések általános leírása.

104. A nyilvántartást az adatvédelmi tisztviselő elektronikus formában vezeti. A nyilvántartásban szereplő adatkezelésekre, adatfeldolgozásokra vonatkozó, a 129-130. pontban felsorolt információkat az adott adatkezelést, adatfeldolgozást végző munkatárs bocsájtja az adatvédelmi tisztviselő rendelkezésére. A nyilvántartásban szereplő adatkezeléseket, adatfeldolgozásokat, valamint az azokkal kapcsolatosan rögzített információkat az adatvédelmi tisztviselő évente felülvizsgálja.

105. Ha az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelés megkezdésétől számított legalább háromévente az Adatkezelő felülvizsgálja, hogy az általa, illetve az Adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. E felülvizsgálat körülményeit és eredményét írásban kell dokumentálni. A felülvizsgálatba az adatvédelmi tisztviselőt be kell vonni, részére a felülvizsgálatot tartalmazó dokumentumot meg kell küldeni.

106. Az Adatkezelő — megkeresés alapján — a NAIH rendelkezésére bocsátja a nyilvántartást.

Érdekmérlegelési teszt, hatásvizsgálat

107. Amennyiben az Adatkezelő által végzett adatkezelés jogalapja a GDPR rendelet 6. cikk (1) bekezdésének f) pontja szerinti jogos érdek, az adatkezelés megkezdése előtt érdekmérlegelési tesztet kell készíteni.

108. Az érdekmérlegelési tesztet az alábbi kérdések mentén kell elkészíteni:

a) Adott célhoz feltétlenül kell-e személyes adatokat kezelni? (Ha enyhébb eszköz alkalmazható ugyanarra a célra, azt kell alkalmazni.)
b) Az adatkezeléshez fűződő jogos érdek pontos meghatározása, pl. személy- és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.
c) Mi az adatkezelés célja, mely személyes adatok mennyi ideig tartó kezelését igényli?
d) Annak meghatározása, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában.
e) Annak meghatározása, hogy miért korlátozza arányosan az adatkezelői jogos érdek az érintetti jogokat.

109. Az érdekmérlegelési tesztet az Adatkezelő munkavállalója az adatvédelmi tisztviselő közreműködésével készíti el, majd elkészültével véleményezésre megküldi az adatvédelmi tisztviselő számára.

110. Az elkészült érdekmérlegelési tesztet adatvédelmi tisztviselő, valamint az Adatkezelő vezetője aláírásával látja el.

111. Ha az adatkezelés valamely különösen új technológiákat alkalmazó — típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, Az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan, egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

112. A hatásvizsgálatot az adott adatkezelést végző munkavállaló köteles elvégezni az adatvédelmi tisztviselő közreműködésével.

113. A hatásvizsgálatot a NAIH által közzétett iránymutatás szerint kell elvégezni.

Kártérítés és sérelemdíj

114. Amennyiben az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni. Amennyiben az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet.

115. Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért és az adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is.

Az adatkezelő mentesül az okozott kárért való felelősség és sérelemdíj megfizetésének kötelezettsége alól, amennyiben bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Nem kell megtéríteni a kárt és nem követelhető sérelemdíj,

amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

116. A kártérítés és sérelemdíj iránti követelések kivizsgálását az adatvédelmi tisztviselő koordinálja.

Záró rendelkezés

117. Ez a Szabályzat az elfogadásával lép hatályba, ezzel egyidejűleg a 2019. december 13-i Adatvédelmi és Adatkezelési Szabályzat hatályát veszti.

118. A Magyar Orvosi Kamara Fogorvosok Területi Szervezete elnöksége a jelen Szabályzatot 2024. április 05-én a 20/2024. (IV.05.) számú határozatával fogadta el.

Magyar Orvosi Kamara
Fogorvosok Területi Szervezete
1068 Budapest, Szondi u. 100.
Telefon: 36-1-353-2188
E-mail: kamara@fogorvos.hu

Belső informatikai rendszerhez való hozzáférési jogosultság

Alulírott, ……., mint a Magyar Orvosi Kamara Fogorvosok Területi Szervezete elnöke/ügyviteli vezetője kezdeményezem a belső informatikai rendszerhez való hozzáférési jogosultság adását az alábbi személy számára, az alábbi tartalommal:

Név: ……
Anyja neve: ……;
Születési hely és idő: ……;
Cím: ……;
Munkaköre: ……;

A Magyar Orvosi Kamara Fogorvosok Területi Szervezetével fennálló jogviszonya minősítése: ……
Jogosultsági szint: ……
Jogosultság időtartama: ……

Budapest, ……..

……
elnök/ügyviteli vezető

Jogosultsági szintet beállítottam, jelszót átadtam.

……
rendszergazda
Dátum: ……

Jelszót átvettem.

……..
felhasználó
Dátum: ……

Jelszót és jogosultságot töröltem.

Indoka: ……

……..
rendszergazda

2. számú melléklet

Adatvédelmi incidenskezelési terv

1. Az incidensminősítés szempontjai

Adatvédelmi incidens bekövetkezésének mindig előfeltétele a biztonság sérülése. Ilyen lehet például – de nem kizárólagosan – személyes adatokat tartalmazó adathordozó (USB, laptop, HDD) elvesztése, ellopása. hacker támadás, jelszó nyilvánosságra kerülése, személyes adatokat tartalmazó dokumentum elveszítése, illetéktelen általi megismerése, jogosulatlanok számára elérhetővé válása.
Adatvédelmi incidens akkor következik be, ha a biztonság olyan sérülése történt meg, 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.

Bizalmasság, sértetlenség, rendelkezésre állás

- Bizalmasság: személyes adatokhoz, illetéktelenek hozzáfértek
- Sértetlenség: személyes adatokat – véletlenül vagy jogellenesen – megváltoztatták, így azok már nem alkalmasak az eredeti cél szerinti kezelésre
- Rendelkezésre állás: a személyes adatokhoz az adatkezelő időlegesen vagy véglegesen nem fér hozzá

Amennyiben a fenti három pont közül bármelyik bekövetkezett adatvédelmi incidensről beszélünk.

Ha a biztonság sérülése megállapítható, de kizárható a személyes adatok sérülése, az nem minősül adatvédelmi incidensnek.

2. Adatvédelmi incidens jelzése

Amennyiben a MOK FTESZ munkavállalója, vagy a MOK FTESZ adatfeldolgozójának alkalmazottja adatvédelmi incidensről, vagy annak bekövetkezését feltételező eseményről szerez tudomást, a következőképpen kell eljárjon:

- A MOK FTESZ munkavállalója az eseményt az arról való tudomásszerzését követően haladéktalanul bejelenti az ügyviteli vezetőnek.
- Amennyiben a MOK FTESZ adatfeldolgozójánál, annak alvállalkozójánál, teljesítési segédjénél történt az MOK FTESZ-t, mint adatkezelőt bármely módon érintő valós, vagy alappal feltételezett adatvédelmi incidens, arról a tudomásszerző haladéktalanul értesíti a ügyviteli vezetőt.
- A MOK FTESZ irodavezetője az adatvédelmi incidensről haladéktalanul értesíti az adatvédelmi tisztviselőt.
- A bejelentő bejelentésében megadja:
    - nevét, e-mail címét, telefonszámát,
    - az esemény megtörténtének és észlelésének időpontját,
    - az esemény leírását, és az azzal összefüggő minden rendelkezésére álló információt,
    - az eseménnyel érintett informatikai rendszer megnevezését,
    - az adatvédelmi incidenssel érintettek feltételezhető számát.
- A bejelentést elektronikus levél formájában kell megtenni, melynek elküldéséről „kézbesítési és olvasási visszaigazolást” kell kérni.

Amennyiben a bejelentő bejelentésének elküldését követő 4 órán belül nem kap olvasási visszaigazolást, az ügyvitelivezetőt telefonon is értesíti. Ha a telefonos értesítési kísérlet sem jár sikerrel, a bejelentő az adatvédelmi tisztviselőt telefonon értesíti.

3. Az adatvédelmi tisztviselő által értesítendők köre

Az adatvédelmi tisztviselő az adatvédelmi incidensről értesíti

- irodavezetőt,
- ügyviteli vezetőt,
- informatikai rendszert vagy eszközt érintő incidens esetén az informatikust.

Az adatvédelmi tisztviselő az általa értesítendőknek megadja a bejelentő nevét, e-mail címét, telefonszámát, az esemény megtörténtének és észlelésének időpontját, az esemény rövid leírását, a rendelkezésre álló információkat, az adatvédelmi incidenssel érintettek feltételezhető számát, valamint azt, hogy érint-e informatikai rendszert az esemény.

4. Az adatvédelmi incidens kezelése

Az adatvédelmi tisztviselő javaslatára az elnök dönt, hogy a tudomására jutott esemény adatvédelmi incidens-e, vagy sem.
Amennyiben az adatvédelmi tisztviselő megítélése szerint a rendelkezésre álló adatok alapján még nem eldönthető, hogy adatvédelmi incidens történt-e vagy sem, további információkat kér a bejelentőtől, a MOK FTESZ más munkavállalójától, az adatfeldolgozótól, annak alvállalkozójától. Az adatvédelmi tisztviselő részére az eseményre vonatkozóan mindenki haladéktalanul köteles a lehető legpontosabb és minden részletre kiterjedő információt megadni.

Adatvédelmi incidens megtörténtekor az adatvédelmi tisztviselő vizsgálatot kezdeményez.

A „Vizsgálati jegyzőkönyv" legalább az alábbiakat tartalmazza:

- Az incidens leírása
- Az incidenssel érintettek száma (a lehető legpontosabban)
- Az incidenssel érintettek köre, kategóriái
- Az incidenssel érintett adatok köre
- Az incidens valószínűsíthető következményei
- Az incidens orvoslására tett intézkedések
- A jegyzőkönyv felvételének helye és ideje

A MOK FTESZ minden adatvédelmi incidenst nyilvántart. Az adatvédelmi tisztviselő vezeti az adatvédelmi incidensek nyilvántartását.
Az adatvédelmi tisztviselő minden adatvédelmi incidensről „Összefoglaló mappá"-t készít, amely minimálisan a következő dokumentumokat tartalmazza:

- Vizsgálati jegyzőkönyv
- Incidens adatlap
- amennyiben az incidens bejelentésre került a Nemzeti Adatvédelmi és Információszabadság Hatóság részére, a bejelentés megtörténtét igazoló dokumentumok
- az orvoslásra tett intézkedések leírása

Az adatvédelmi incidens dokumentálása egyedi iktatási számon történik.

Adatvédelmi incidens bejelentése a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) részére

Amennyiben az adatkezelési incidens az érintett személyek jogaira és szabadságaira kockázattal járhat, a MOK FTESZ– az adatvédelmi tisztviselő útján – az adatvédelmi incidenst a tudomásszerzéstől számított 72 órán belül bejelenti a NAIH-nak.

Az adatvédelmi incidens bejelentéséről az adatvédelmi tisztviselő javaslatára az elnök dönt.

Az adatvédelmi incidens bejelentésére a NAIH által közzétett „Incidensbejelentő" formanyomtatványt kell használni.

Amennyiben az incidensről 72 órán belül nem áll rendelkezésre minden adat, de az a meglévő információk alapján az érintett személyek jogaira és szabadságaira nézve kockázattal jár, az incidenst akkor is jelenteni kell a meglévő

adatokkal, az alábbi kiegészítéssel: *„A MOK FTESZ még nem rendelkezik az incidensről teljeskörű információkkal, de a vizsgálat folyamatban van. A lehető leghamarabb csatoljuk a hiányzó adatokat.”*

5. Érintettek értesítése

Amennyiben az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, arról a MOK FTESZ indokolatlan késedelem nélkül tájékoztatja az érintetteket.
Amennyiben az incidenssel érintettek elérhetősége rendelkezésre áll, őket közvetlenül kell értesíteni. Amennyiben a közvetlen tájékoztatás aránytalan erőfeszítést tenne szükségessé, akkor az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni.

Az érintettekkel közölni kell minimálisan az alábbiakat:

- az adatvédelmi tisztviselő és/vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit
- az incidensből eredő lehetséges következményeket
- a MOKFTESZ által megtett intézkedéseket

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

a)
- az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és
- ezért az érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára ezek értelmezhetetlenné teszik az adatokat;

b)
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy a magas kockázat a továbbiakban valószínűsíthetően nem valósul meg.

A MOK FTESZ mindent megtesz az adatvédelmi incidensek elkerülése érdekében. Amennyiben ilyen esemény mégis bekövetkezne, a lehető leghamarabb megtesszük mindazokat az intézkedéseket, melyek eredményeképpen az érintettek jogait és szabadságait veszélyeztető felmerült kockázatok megszüntethetők.