

MAGYAR ORVOSI KAMARA
FOGORVOSOK TERÜLETI SZERVEZETE

Adatvédelmi és Adatkezelési Szabályzat ¹

2019. év



Dr. Hermann Péter
elnök

TARTALOMJEGYZÉK

I. FEJEZET ÁLTALÁNOS RENDELKEZÉSEK

II. FEJEZET A SZEMÉLYES ADATOK VÉDELME

II/A. FEJEZET SZERVEZETI ADATKEZELÉS

II/B. FEJEZET FOGLALKOZTATÁSI ADATKEZELÉS

II/C FEJELEZET ETIKAI ÜGYEK ADATKEZELÉSE

III. FEJEZET AZ ADATVÉDELEM SZERVEZETE

IV. FEJEZET A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA

V. ZÁRÓ RENDELKEZÉS

MELLÉKLETEK:

1. MELLÉKLET TITOKTARTÁSI NYILATKOZAT

2. MELLÉKLET BELSŐ INFORMATIKAI RENDSZERHEZ HOZZÁFÉRÉSI JOGOSULTSÁG

3. MELLÉKLET HOZZÁJÁRULÁS KÜLÖNLEGES ADATOK KEZELÉSÉHEZ

4. MELLÉKLET KÖZÉRDEKŰ ADATSZOLGÁLTATÁSI NYILVÁNTARTÁS MINTA

5. MELLÉKLET ADATVÉDELMI INCIDENSKEZELÉSI TERV

A Magyar Orvosi Kamara Fogorvosok Területi Szervezete, az egészségügyben működő szakmai kamarákról 2006. évi XCVII. törvényben (továbbiakban: Ekt.) meghatározott feladatainak ellátása és tevékenysége során keletkező, valamint a tagok és más érintettek által szolgáltatott adatok védelme érdekében, figyelemmel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (3) bekezdésére, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) szerint) az alábbi Adatkezelési és Adatvédelmi Szabályzatot hozza létre:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályozás célja

A jelen szabályzat célja, hogy meghatározza a Magyar Orvosi Kamara Fogorvosok Területi Szervezete (a továbbiakban: Szervezet) által folytatott adatkezelés jogszerű rendjét, valamint biztosítsa az adatok biztonságát, érvényre juttassa az adatvédelmi szabályokat és megakadályozza az adatokhoz való jogosulatlan hozzáférést.

A szabályzat célja továbbá a hivatali ügyintézés során az érintettek személyes adatainak védelme, illetve a közérdekű adatok nyilvánosságának biztosítása.

2. A szabályzat hatálya

2.1 Személyi hatálya kiterjed a Szervezet elnökére, testületeire, azok tisztségviselőire, tagjaira, az ügyviteli szervezetre és annak munkatársaira, valamint a Szervezettel munkaviszonyban álló személyekre, valamint azokra a megbízási vagy más szerződés alapján a Szervezettel jogviszonyban álló személyekre és szervezetekre, akik az adatkezelés és adatfeldolgozás során feladatot teljesítenek.

2.2. Tárgyi hatálya kiterjed a Szervezetenél személyes adatokkal végzett valamennyi tevékenységre.

3. Alapelvek

3.1. Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és jogszerűnek kell lennie.

3.2. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

3.3. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

3.4. Az adatkezelések során biztosítani kell, az adatkezelés átláthatóságát. Az érintetteknek nyújtandó tájékoztatóknak rövidnek, tömörnek, könnyen érthetőnek kell lennie.

3.5. Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

3.6. Kizárólag olyan személyes adat kezelhető, amely az adatkezelés szempontjából szükséges, releváns és megfelelő,

4. Fogalmak

4.1. A vonatkozó jogszabályok alapján:

1. érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;
2. azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
3. személyes adat: az érintettre vonatkozó bármely információ;
4. különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,
5. genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;
6. biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;
7. egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
8. bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
9. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

10. közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
11. hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
12. adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
13. közös adatkezelő: az az adatkezelő, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtattja végre az adatfeldolgozóval;
14. adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
15. adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
16. közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;
17. nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;
18. adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
19. adatkezelés korlátozása: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;
20. adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
21. adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;
22. adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;
23. adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
24. adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

25. adatállomány: az egy nyilvántartásban kezelt adatok összessége;
26. harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy 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 irányuló műveleteket végeznek;
23. EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;
24. harmadik ország: minden olyan állam, amely nem EGT-állam;

4.2. A jelen szabályzat alkalmazásában:

szervezeti egység: ügyviteli szervezet, elnökség, etikai bizottságok

I. SZEMÉLYES ADATOK VÉDELME

5. Általános szabályok

5.1. A személyes adatok védelméért, az adatkezelés jogszerűségéért a Szervezet valamennyi szervezeti egységének vezetője, valamint az adatkezelést végző ügyintézője és ügykezelője felelős.

5.2. A Szervezetben kezelt személyes adatok védelméről az adatvédelemmel kapcsolatos szabályoknak a foglalkoztatottak általi megismeréséről és betartásáról a Szervezet valamennyi szervezeti egységének vezetője gondoskodni köteles. A vonatkozó szabályok megismertetését tényét írásban rögzíteni kell, mely dokumentumot az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

5.3. A Szervezet a személyes adatok kezelésének módjáról és elveiről a hatályos jogszabályok értelmében adatkezelési tájékoztatót köteles szerkeszteni, amelyben közérthetően leírja az érintetti jogokat, közzéteszi az adatfeldolgozók listáját és az adatvédelmi tisztviselő elérhetőségét. Az aktuális adatkezelési tájékoztatót a Szervezet a honlapján közzéteszi, a székhelyén az ügyfélfogadásra szolgáló irodában kinyomtatva, jól látható és bárki számára hozzáférhető helyen elhelyezi, illetve bárkinek kérésére e-mail útján megküldi.

5.4. Az érintett kérelmére, kezdeményezésére indult hatósági eljárásban az eljárás lefolytatásához szükséges személyes adatok tekintetében, az érintett kérelmére indult más ügyben az általa megadott személyes adatok tekintetében az érintett hozzájárulását vélelmezni kell az adott ügyfajtájára vonatkozó feltételek szerint.

5.5. A különleges adatok kezeléséhez az érintett 1. melléklet szerinti, illetőleg jegyzőkönyvi hozzájárulását kell kikérni, kivéve, ha hozzájárulását, különleges adatát írásbeli beadványban maga az érintett közölte. Amennyiben a különleges adatok kezelését jogszabály írja elő vagy ha a különleges adatok kezeléséhez történt hozzájárulást jogszabály alapján vélelmezni kell, az írásbeli hozzájárulás bekérése nem szükséges.

5.6. Különleges adatok kezelésével járó ügyekben – a jogszabályokban és jelen Szabályzatban foglaltakon túl is – fokozott gondossággal kell eljárni.

5.7. Az ügyintézés során kizárólag azokat a személyes adatokat szabad felvenni, amelyek az ügy szempontjából feltétlenül szükségesek vagy amelyek felvételére jogszabály kötelezi a Szervezetet.

5.8. Az érintettel az adat felvétele előtt közölni kell az adatkezelés célját, valamint azt, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt.

5.9. A Szervezet kezelhet személyes adatot kamarai tagok esetében az Ekt-ban foglalt feladatainak ellátása érdekében, illetve egyéb esetben az az Infotv. 5. § bekezdésében foglaltak fennállása esetén is.

5.10. Az adatfelvétel és a további adatkezelés folyamán ügyelni kell a személyes adatok pontosságára, teljességére és időszerűségére, hogy emiatt az érintettek jogai ne sérülhessenek.

6. Betekintésre vonatkozó szabályok

6.1. Az ügyintézőnél, vagy az irattárban lévő iratba az ügyintézőn és az adott szervezeti egység vezetőjén kívül más személy – az érintett törvény szerinti betekintési jogán túl – csak akkor tekinthet be, ha ezt törvény lehetővé, vagy a hivatali tevékenységével összefüggő feladatellátás szükségessé teszi.

6.2. Az érintett betekintési jogának gyakorlása során úgy kell eljárni, hogy ez által mások jogai ne sérülhessenek (a más személyre vonatkozó személyes, vagy védett adatokat adott esetben ki kell takarni vagy más módon felismerhetetlenné tenni). Ugyanígy kell eljárni a másolat, kivonat készítésekor is.

7. Adatbiztonsági rendszabályok

7.1. A Szervezet foglalkoztatottja a nála lévő, valamint a vonatkozó jogszabályok és jelen Szabályzat előírásai alapján személyes adatnak minősülő adatokat tartalmazó iratokat köteles munkaidőn túl – és amelyeket lehetséges munkaidőben is – szekrényébe zárva tartani, az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak tartama alatt tárolhatók.

7.2. Az iratok elzárásáért az az ügyintéző felelős, akinél azok a munkaidő befejezésekor találhatók.

7.3. Az egyéb szempontokon túl adatvédelmi megfontolásból azokat a helyiségeket, ahol közös használatú nyomtató vagy másológép üzemel, az adatbiztonsági követelmények figyelembevételével kell használni.

7.4. Az egyéb szempontokon túl adatvédelmi megfontolásból azokat a szobákat, helyiségeket, ahol számítógép, munkaállomás üzemel, úgy kell használni, hogy az megfeleljen az adatvédelmi, tűzrendészeti és informatikai biztonsági követelményeknek. Az ügyintéző 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 munkaállomást – a folyamatosan bekapcsolva, illetve online tartandó munkaállomások kivételével – kikapcsolni, az ajtót bezárni.

7.5. A tűzrendészeti előírásokat be kell tartani. A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a Szervezet székhelye szerinti tűz- és munkavédelmi előírások tartalmazzák.

7.6. Személyes adatokat is tartalmazó iratot a Szervezet irodáiból kivinni – munkaköri feladat ellátásának kivételével – csak a közvetlen felettes vezető engedélyével lehet. Az ügyintéző ez esetben is köteles gondoskodni arról, hogy az ne vesszen el, ne rongálódjon vagy semmisüljön meg és tartalma illetéktelen személy tudomására ne jusson. Amennyiben személyes adatokat is tartalmazó irat - a jelen bekezdés szerint - a Szervezet irodáiból kivitelre kerül, úgy annak kiviteléről és visszahozataláról feljegyzést kell készíteni.

7.7. A számítástechnikai eljárás során keletkezett munkapéldányt, illetőleg rontott vagy egyéb okból feleslegessé vált iratokat haladéktalanul meg kell semmisíteni iratmegsemmisítő géppel.

7.8. A személyes adatok – titkosítás nélkül - külső adathordozón (CD, DVD, pendrive stb.) nem rögzíthetők.

7.9. Az iratok telefaxon, az adatok telefonon, illetve egyéb elektronikus úton csak kellő körültekintéssel és kizárólag a Szervezet technikai eszközeinek igénybevételével továbbíthatók.

7.10. Az adatvédelemmel összefüggő számítógépes adatkezelés szabályairól, így különösen az archiválás, mentés, törlés rendjéről, továbbá az egyes programok és belső tárhelyek tekintetében a hozzáférési és a betekintési jogosultságokról és az ehhez kapcsolódó ügyintézői jelszavakról a Rendszerleírás és belső vezetői utasítás rendelkezik.

8. Adatvédelmi incidens

8.1. Adatvédelmi incidens vagy olyan esemény megtörténése esetén, amely esetlegesen adatvédelmi incidens lehet a jelen szabályzat 5. számú mellékletét képező „Incidenskezelési terv” rendelkezéseinek megfelelően kell eljárni.

8.2. A Szervezet köteles incidens nyilvántartást vezetni, amelybe minden megtörtént incidenst fel kell vezetni. A nyilvántartás részét képezi az incidenskezelési terv mellélete szerinti mintatáblázat, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, várható hatásait és a megtett intézkedéseket, valamint GDPR-ban meghatározott egyéb adatokat.

9. Informatikai védelem

9.1. A személyes adatokat tartalmazó számítógépes információs rendszer védelme érdekében gondoskodni kell az információs rendszerben az adatkezelés biztonságáról, a működtetés rendjéről. Alapvető biztonsági intézkedésként a szervezet munkaállomásainak hardver- és szoftver eszközeit rendszeres vírusvédelemmel, és folyamatos program frissítéssel, valamint rendszer tűzfallal, napi mentési és naplózási mechanizmussal kell ellátni.

9.2. A számítógépes információs rendszerrel kapcsolatos adatbiztonságra, a fizikai biztonságra, az üzemeltetés és a technikai biztonságra, továbbá az információtovábbítás rendjére vonatkozó részletes szabályokat a Rendszerleírás és a vonatkozó vezetői utasítás tartalmazza.

9.3. A belső informatikai rendszer használatát személyre szóló felhasználó névvel és ehhez rendelt külön jelszavas belépéssel kell védeni. Belépés után a számítógépet nem lehet felügyelet nélkül hagyni, a számítógéphez, illetve az ott tárolt adatokhoz való illetéktelen hozzáférést meg kell akadályozni.

9.4. A felhasználók részére jelszó kiadása az elnök vagy az ügyviteli vezető írásbeli döntése alapján lehetséges, amely tartalmazza a felhasználó nevét, a Szervezettel fennálló jogviszonya minősítését, a kért jogosultsági szintet és, hogy mennyi időre szóljon a jogosultság, amennyiben az előre tudható.

9.5 A jogosultság beállításának és a jelszó kiadásának tényét rögzíteni kell, a dokumentum gondosan zárható, biztonságos helyen őrizendő.

9.6. A kiadott jelszó a munkaviszony vagy a megbízás időtartamára érvényes. Az érvényesség lejártakor az elnök, illetve az ügyviteli vezető írásban tájékoztatja a rendszergazdát, aki törli a jogosultságot. Ugyancsak törölni kell a jogosultságot, ha a felhasználó 3 hónapnál hosszabb időre nem veszi igénybe az informatikai rendszert.

10. Törlésre vonatkozó szabályok

10.1. Olyan, személyes adatokat tartalmazó iratokat, amelyekre nézve az adatkezelés célja már megszűnt, jogszabályban vagy az iratkezelésre alkotott belső szabályzatban foglalt időtartam leteltét követő év május 31. napjáig selejtezni kell, vagy átadni az őrzésre jogosult szervnek.

11. Egyes nyilvántartások

11.1. Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot a szervezeti egységek vezetőjének személyre bontottan meg kell határozni és az időszerű állapotnak megfelelő nyilvántartásukról gondoskodnia kell.

12. Adattovábbítás, az adatkezelések összekapcsolása

12.1. A személyes adatokat továbbítani, vagy adatszolgáltatást teljesíteni, illetőleg a különböző adatkezeléseket összekapcsolni csak akkor lehet, ha ahhoz az érintett hozzájárult, vagy törvény ezt előírja, illetve megengedi. Harmadik országba történő adattovábbítás esetén az Infotv. és a GDPR vonatkozó rendelkezéseit kell alapul venni.

12.2. Az adattovábbítást a 2.-3. melléklet szerinti adattartalomra kiterjedően regisztrálni, azaz naplózni kell (adattovábbítási- és adatszolgáltatási nyilvántartás), annak érdekében, hogy megállapítható legyen milyen adat, kinek, milyen felhatalmazottság alapján, mikor került továbbításra vagy kiszolgáltatásra (pl. belföldi jogsegély, stb.).

13. Adattovábbítás

13.1. Az érintettet az adattovábbításra vonatkozó törvényi felhatalmazás hiányában nyilatkoztatni kell – különleges adatai tekintetében írásban – a kérelmére indult eljárásban, hogy hozzájárul-e személyes adatainak a továbbításához, ha ügye elintézéséhez más szerv megkeresése szükséges.

13.2. Személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – továbbíthatók olyan adatkezelőhöz és adatfeldolgozóhoz amely ezen adatokkal kapcsolatban a Szervezet feladat- és hatásköréhez tartozó további feladatokat lát el. Ebben az esetben a MOK FTESZ az ezen feladatot ellátóval köteles adatfeldolgozási szerződést kötni, amely szerződésben minimálisan a GDPR-ban előírt kötelező tartalmi elemeinek szerepelnie kell.

II/A. SZERVEZETI ADATKEZELÉS

14. Általános szabályok

14.1. A tisztségviselők tisztségük elnyerését, a testületi tagok megválasztásukat, a munkavállalók munkaviszonyuk kezdetét, a megbízási szerződéses vagy vállalkozói jogviszonnyal rendelkezők a szerződés hatályba lépését követően haladéktalanul kötelesek az adatvédelmi előírások betartására is kiterjedő, valamint titoktartási kötelezettség vállalásáról szóló nyilatkozatot kitölteni. Jelen szabályzat személyi hatálya alá tartozók kötelesek a feladatkörük ellátása során tudomásukra jutott személyes adatot és üzleti titkot megőrizni.

14.2. A Szervezet belső informatikai rendszerének valamennyi felhasználója felelősséggel tartozik azért, hogy a kiadott személyes jelszót más számára nem adja át, más személyekkel nem osztja meg. Amennyiben felmerül a gyanú, hogy jelszava illetéktelen személy tudomására jutott, ezt haladéktalanul köteles az ügyviteli vezetőn keresztül a rendszergazdának írásban jelezni, aki azonnal törli a jelszót és az ahhoz tartozó jogosultságot.

14.3. Bármely számítógép vírusfertőzésének gyanúja esetén a rendszergazdát haladéktalanul értesíteni kell, majd az ő előírásai szerint kell eljárni.

15. Tagnyilvántartás, szabályzat személyi hatálya alá tartozók személyi adatai

15.1. A tagnyilvántartás vezetése során a kamara tagjainak a személyi iratait és adatait a vonatkozó jogszabályoknak megfelelően kell kezelni.

15.2. A tagnyilvántartás során kezelt személyes adatok tekintetében a Magyar Orvosi Kamara és a MOK FTESZ közös adatkezelők.

15.3. Tisztségviselőkről, testületi tagokról és munkavállalókról csak a tisztséggel, illetve a munkaviszonnyal összefüggő adat tárolható. Jelen pont hatálya alá tartozóktól csak olyan nyilatkozat, vagy adatlap kitöltése kérhető, amely személyiségi jogait nem sérti.

15.4. A személyi iratokat a Szervezet hivatalos helyiségében, zárható szekrényben kell tárolni, megakadályozva, hogy illetéktelenek hozzájuthassanak. A személyi iratokat az illetékes ügyintéző, valamint az ügyviteli vezető a munkavégzéséhez szükséges mértékben

használhatja. Az iratokba ezen kívül csak a munkáltatói jogok gyakorlójának van betekintési joga.

15.5. A tisztséggel, tagsággal vagy munkaviszonnyal kapcsolatos személyi irat, dokumentum kizárólag személyesen, vagy teljes bizonyítóerejű magánokiratba foglalt meghatalmazással vehető át, illetve „saját kezébe” jelzéssel ellátott küldeményként az érintett lakcímére postázandó, amennyiben szükséges.

16. Gazdasági tevékenységhez kapcsolódó adatkezelés

16.1. A Szervezet gazdasági tevékenysége során tudomására jutó üzleti titok megőrzéséről, a gazdasági, pénzügyi adatok jogszabályoknak megfelelő kezeléséről gondoskodik. Így különösen megtartja a vele szerződésben álló vagy részére ajánlatot küldő jogi és természetes személyek üzleti titkait és a jogszabályoknak megfelelően kezeli a tudomására jutott személyes adatokat.

16.2. Az egyes szerződések megszűnését, az ajánlatok visszautasítását, vagy a gazdasági cél megvalósulását követően a Szervezet gondoskodik a pénzügyi, gazdasági és személyes adatok megsemmisítéséről.

II/B. A FOGLALKOZTATÁS ADATVÉDELMI SZABÁLYAI

17.1. E fejezet rendelkezései szerint kell ellátni a Szervezettel munkaviszonyban, megbízási jogviszonyban vagy egyéb munkavégzésre irányuló jogviszonyban álló személyek (a továbbiakban együtt: munkavállalók) személyi adatainak kezelését.

17.2. A személyes, illetve a személyügyi adatok (személyi irat) nyilvántartásának alapszabálya, hogy a munkavállalókról csak a munkaviszonnyal összefüggő adatokat szabad tárolni, illetve azokat az adatokat, amelyek kezeléséhez írásban kifejezetten hozzájárult.

17.3. Az álláspályázatokra beérkező dokumentumokban szereplő adatok esetében az érintett hozzájárulását vélelmezni kell. Az egyes álláspályázatokra beérkező dokumentumokat a pályázat lezárását követő 180 nap elteltével meg kell semmisíteni.

17.4. Minden munkavállalónak joga van megismerni a személyével összefüggésben tárolt adatokat.

17.5. A munkavállalótól csak olyan nyilatkozat vagy adatlap kitöltése kérhető, amely személyiségi jogait nem sérti. Az adatok harmadik személlyel, különösen a munkaviszony megszűnése után az új munkáltatóval csak abban az esetben közölhetők, ha a munkavállaló ezt kifejezetten kéri.

17.6. A személyi iratokat a Szervezet hivatalos helyiségében, zárt szekrényben kell tárolni, megakadályozva, hogy illetéktelenek hozzájuthassanak, az informatikai tárhelyen lévő adatokat pedig titkosítva kell kezelni. A személyi iratokat az illetékes ügyintéző a munkavégzéséhez szükséges mértékben használhatja. Az iratokba - ezen kívül - csak a munkáltatói jogkör gyakorlójának van betekintési joga.

17.7. A munkáltató a munkabérfizetéssel kapcsolatos kötelezettségei teljesítése céljából a munkavállaló személyes adatait a mindenkori bérszámfejtési tevékenységgel megbízott cég

részére jogosult átadni.

A bérszámfejtéssel megbízott szervezetnek csak azok az adatok továbbíthatók, amelyek a bérszámfejtéssel kapcsolatos feladatok ellátását szabályozó jogszabályok szerint nélkülözhetetlenek az érintett munkavállaló jövedelmének számfejtéséhez, valamint a társadalombiztosítással, családi pótlékkal, személyi jövedelemadóval összefüggő bevallások benyújtásához szükségesek. Az előzőekben meghatározottakon kívüli adatok továbbítását a bérszámfejtéssel megbízott szervezet kezdeményezésére is meg kell tagadni. A bérszámfejtéssel megbízott, mint adatfeldolgozó felelős az átadott adatok védelméért, kezelésük jogszerűségéért.

17.8. A személyi iratok körébe sorolandók különösen az alábbiak:

- a) a munkaszerződés, az önéletrajz, a bizonyítványok
- b) a jogviszonnyal összefüggő egyéb iratok, (adóbevallás, fizetési letiltás, kedvezményjog stb.),
- c) a foglalkoztatott saját kérelmére kiállított, vagy önként átadott egyéb iratai.

17.9. A személyi iratra csak olyan adat és megállapítás vezethető, amelynek alapja közokirat vagy a foglalkoztatott írásbeli nyilatkozata, a munkáltatói jogkör gyakorlójának írásbeli rendelkezése, bíróság vagy más hatóság döntése, vagy jogszabályi rendelkezés.

17.10. A személyi iratokban feltüntetett adatokat elsősorban az érintett szolgáltatja, másodsorban hatósági nyilvántartás vagy korábbi foglalkoztató közvetíti.

17.11. A munkavállaló írásbeli kérelmére olyan adat is kezelhető, amelynek átadására az érintett törvényi előírás alapján nem köteles. Ezek az adatok azonban csak az érintett által meghatározott célra használhatók fel, illetve csak írásbeli hozzájárulásával továbbíthatók más szerv részére. Az említett adatokat elkülönítetten kell kezelni, és az azokban szereplő személyazonosító adatokat a foglalkoztatott kérésére haladéktalanul törölni kell a nyilvántartásból.

17.12. A Szervezetnél keletkezett, illetve a Szervezethez érkezett vagy leadott személyi iratok iktatása, kezelése személyenként és évenként külön főszámon, ezen belül egy személyre vonatkozóan, keletkezésük sorrendjében alszámokon, a számítógépes iktatórendszeren belül, az ügyiratkezelés szabályai szerint történik.

A személyi iratok iktatása és irattározása során gondoskodni kell arról, hogy az iratba jogosulatlan személy ne tekinthessen be.

17.13. A foglalkoztatott személyes adatait tartalmazó dokumentumokat a jogviszony megszűnését követően is meg kell őrizni, a hatályos jogszabályokban foglalt őrzési idő lejártáig.

17.14. A Szervezet a vonatkozó jogszabályok valamint a munka törvénykönyvéről szóló 2012. évi I. tv. (továbbiakban: Mt.) vonatkozó rendelkezéseit figyelembe véve, a munkavállalók adatait az alábbi módon kezeli:

- a) a Szervezet foglalkoztatottjaira vonatkozó tény, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy az érintett munkavállaló hozzájárulásával közöl;
- b) a Szervezet a munkaviszonyból származó kötelezettségek teljesítése céljából a munkavállalók személyes adatait – az adatszolgáltatás céljának megjelölésével, a törvényben meghatározott körben – adatfeldolgozó számára átadhatja, ennek tényéről az érintett

munkavállalókat a munkaszerződés megkötésekor, egyéb egyedi esetben pedig az adattovábbítást megelőzően előzetesen tájékoztatja;

c) a Szervezet a munkavállalókra vonatkozó adatokat statisztikai célú felhasználásra munkavállalók hozzájárulása nélkül, személyazonosításra alkalmatlan módon is átadhat.

17.15. Munkaszerződés esetén kezelt személyes adatok:

- a) név, születési év, hó, nap, hely,
- b) anyja neve,
- c) lakcím, lakcímváltozás időpontja,
- d) adóazonosító jel,
- e) TAJ szám,
- f) TB kiskönyvben található személyes adatok
- g) magán-nyugdíjpénztári tagságra vonatkozó adatok
- h) önéletrajz és az abban szereplő elérhetőségi adatok (pl. e-mail cím, telefonszám)
- i) iskolai végzettséget igazoló bizonyítványok adatai
- j) szakirányú képesítést/szakképzettséget/szakképesítést igazoló bizonyítványok adatai, az ezen igazoló okiratot kibocsátó intézmény(ek) neve és az okirat(ok) száma,
- k) idegen nyelv ismeretét igazoló bizonyítványok adatai
- l) munkaviszony igazolás (ok),
- m) kiskorú hozzátartozó személyes adatai: születési hely, idő, anyja neve, TAJ-száma, születési anyakönyvi kivonata, egészségügyi adatok
- n) pótszabadságra jogosító igazolás,
- o) bankszámlaszám
- p) mobiltelefonszám
- r) privát e-mailcím.
- s) munkavállalóra és hozzátartozóira vonatkozó egészségügyi adatok
- t) házastársra vonatkozó személyes adatok

17.16. A munkaviszony megszűnésekor elkészített igazolásokon a munkavállaló nagyon sok személyes adata szerepel. Ezért az ilyen igazolás személyesen, illetve teljes bizonyító erejű magánokirat formájában készült meghatalmazással vehető át, vagy saját kezébe jelzéssel ellátott levélben a munkavállaló lakcímére vagy az általa megjelölt levelezési címre kell postázni. Bármilyen egyéb kereseti- vagy béradatot statisztikai felhasználásra úgy lehet átadni, hogy általa az érintett személy ne legyen azonosítható, kivéve, ha a jogszabály másképpen rendelkezik.

17.17. Megbízási szerződés esetén kezelt személyes adatok:

- a) név (ideértve jogi személy neve is),
- b) születési év, hó, nap, hely,
- c) anyja neve,
- d) lakcím
- e) személyi igazolvány száma
- f) adóazonosító jel
- g) TAJ szám
- h) bankszámlaszám
- i) e-mail cím,
- j) telefonszám

II/C. ETIKAI ÜGYEK ADATKEZELÉSE

18.1. Az etikai ügyek adatkezelése során kizárólag a Szervezet által megbízott etikai ügyintéző, valamint az illetékes etikai bizottsági tagjai jogosultak az adatokhoz való hozzáféréshez. Az etikai bizottságok tagjai és ügyintézői titoktartási nyilatkozatot kötelesek aláírni a megbízási jogviszonyuk kezdetekor.

18.2. Etikai eljárás során az érintettek személyes adatain nagy számban előfordulhatnak különleges adatok, egészségügyi adatok, ezért fokozottabb biztonsági előírások vonatkoznak az etikai ügyek során megvalósuló adatkezelésre.

18.3. A betekintés joga kizárólag az érintett és képviselőjét – és csak a rá vonatkozó terjedelemben -, valamint az adott etikai ügyintézőt és az etikai bizottságok tagjait illeti meg.

18.4. A megbízott etikai ügyintéző köteles az etikai ügyeik adatait és iratait fizikailag elkülönítve, zárt helyen tárolni, valamint az ügyintéző részére egyedileg és kizárólagos hozzáféréssel kialakított informatikai tárhelyen és a számítógépen, egyéb helyen lévő etikai ügyek dokumentumait titkosítani.

18.5. Az e fejezetben nem részletezettek tekintetében, az etikai ügyekre adatkezelésére a jelen szabályzatban foglaltak irányadók.

III. AZ ADATVÉDELEM SZERVEZETE

19. A Szervezet vezetősége

19.1. A Szervezet elnöke az adatvédelmi szabályok érvényesülése körében az alábbi feladat- és hatáskörökkel rendelkezik:

- a) felügyeli a Szervezet adat- és titokvédelmi tevékenységét, felelős az adat- és titokvédelmi szabályok betartásáért;
- b) rendkívüli ellenőrzést engedélyez,
- c) kivizsgálhatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről;
- d) megállapítja a belső informatikai rendszerhez való hozzáférési jogosultságot (amennyiben szükséges, annak szintjét) és a rendszer használatára vonatkozó jelszó kiadásáról rendelkezik,
- e) megbízza a Szervezet adatvédelmi tisztviselőjét.

19.2. A Szervezet testületeinek elnökei az adatvédelmi szabályok érvényesülése körében az alábbi feladat- és hatáskörökkel rendelkeznek:

- a) felügyelik az irányításuk alá tartozó testületnél folytatott tevékenységgel összefüggő adat- és titokvédelmi előírások teljesülését, felelősek az adat- és titokvédelmi szabályok betartásáért.
- b) A szervezeti egységek vezetői a hozzájuk érkezett, az érintett kezelt adataira vonatkozó, valamint a közérdekű adat megismerése iránti kérelmekről, az esetleges elutasításról tájékoztatják a Szervezet ügyviteli vezetőjét.

19.3. A Szervezet elnöksége az adatvédelmi szabályok érvényesülése körében az alábbi feladat- és hatáskörökkel rendelkezik::

- a) elfogadja a Szervezet belső adatkezelési és adatvédelmi szabályzatát és annak módosítási javaslatait

20. Adatvédelmi tisztviselő

20.1. A Szervezetben kezelt személyes adatok védelme érdekében a Szervezet által kinevezett és megbízott adatvédelmi tisztviselő köteles eljárni a jogszabályok és a Szervezet által vele kötött megbízási szerződésben foglaltaknak megfelelően. A Szervezet által megbízott adatvédelmi tisztviselő eljárása során felhívja az Ügyviteli vezető figyelmét az előírások betartására és az egyes az adatkezeléssel kapcsolatos feladatok teljesítésére.

20.2. Adatvédelmi tisztviselővé – feladatai, hatásköre és felelőssége pontos meghatározásával – írásban megbízott, jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő felsőfokú végzettségű személy jelölhető ki.

20.3. Az adatvédelmi tisztviselő kötelezettségei

- a) közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- b) konkrét ügyekben felmerülő igények alapján adatvédelmi kérdésekben – ésszerű és elvárható határidőn belül – segítséget nyújt a szervezeti egységek munkatársai részére,
- c) ellenőrzi a Szervezet szervezeti egységeinél az adatkezelésre vonatkozó jogszabályok, valamint a jelen Szabályzat rendelkezéseinek betartását,
- d) javaslatot tesz a szervezeti egységek vezetőinek, ha az adatbiztonság érdekében intézkedés meghozatalát látja szükségesnek,
- e) kivizsgálja és intézi a hozzá érkező bejelentéseket,
- f) a személyes adatok kezelése és védelme érdekében javaslatot tesz a belső adatkezelési és adatvédelmi szabályzat tartalmára, jogszabályváltozás miatt vagy más fontos okból történő módosítására, kiegészítésére
- g) koordinálja az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítását, módosításait,
- h) tájékoztatja az adott szervezeti egység vezetőjét a tudomására jutott, a feladatkörében felmerült bármely adatvédelmi problémáról, esetleges állásfoglalásról vagy más, az adatvédelemmel kapcsolatos egyéb kérdésről,
- i) gondoskodik az adatvédelmi ismeretek oktatásáról.

21. Ügyviteli vezető

21.1. Az adatvédelem körében az ügyviteli vezető kötelezettsége:

- a) felügyeli az ügyviteli szervezet adat felügyeli az ügyviteli szervezet adat- és titokvédelmi tevékenységét, felelős az adat- és titokvédelmi szabályok betartásáért.
- b) közreműködik az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- c) ellenőrzi a Szervezetben belül az Info tv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat rendelkezéseinek a megtartását;
- d) a Szervezethez érkezett adatvédelmi tárgyú bejelentéseket, megkereséseket megvizsgálja és szükség esetén továbbítja azokat az adatvédelmi tisztviselőnek
- e) az adatvédelmi tisztviselő javaslata alapján az elnökség elé terjeszti elfogadásra a belső adatkezelési és adatvédelmi szabályzatot és annak módosítási javaslatait
- f) folyamatosan ellenőrzi az ügyviteli szervezetben belül az adatvédelmi jogszabályok és a belső szabályzat érvényesülését
- g) közreműködik az adatkezelési nyilvántartás vezetésében
- h) gondoskodik a titoktartási kötelezettség vállalásáról szóló nyilatkozatok (2. számú melléklet) érintettek általi kitöltetéséről, valamint annak az érintett személyi

- anyagában, illetve az irattárban történő elhelyezéséről;
- i) gondoskodik a belső informatikai rendszerhez való hozzáférési jogosultság (3. számú melléklet) dokumentálásáról és biztonságos helyen történő őrzéséről;
 - j) rendszeresen kapcsolatot tart az adatvédelmi tisztviselővel, részére szükség szerint adatot szolgáltat, információt nyújt a Szervezet adatkezeléséről

22. Rendszergazda

22.1. A rendszergazda

- a) folyamatosan ellenőrzi a jogosultsági rendszert, gondoskodik az informatikai rendszer külső támadás elleni védelme ellenőrzéséről, az informatikai eszközök rendeltetésszerű használatáról és folyamatos üzemképességéről, valamint az adatbiztonsági előírások teljesüléséről;
- b) elektronikusan rögzített adatokról rendszeresen és tervszerűen biztonsági mentéseket, archiválást végez a teljes adatbázisra nézve olyan gyakorisággal, hogy a lehető legkevesebb adatvesztés mellett bármikor folytatható legyen az informatikai programok használata;
- c) a számítógépeket és az adatbázist tűzfallal és vírusvédelmi programmal is védi;
- d) az elnök vagy az ügyviteli vezető kezdeményezésére belépési jelszót ad ki az informatikai rendszer használatára vonatkozóan.

22.2. A tevékenysége során a tudomására jutott személyes adatokkal kapcsolatban az adatfeldolgozási szerződés rendelkezéseinek megfelelően köteles eljárni.

23. Honlap és levelező rendszer üzemeltető

23.1. Az üzemeltető gondoskodik a honlap és a levelező rendszer külső támadás elleni védelme ellenőrzéséről, folyamatos üzemképességéről, valamint az adatbiztonsági előírások teljesüléséről, valamint a levelezőprogramot védi a kéretlen elektronikus üzenetektől is.

23.2 A tevékenysége során a tudomására jutott személyes adatokkal kapcsolatban az adatfeldolgozási szerződés rendelkezéseinek megfelelően köteles eljárni.

IV. A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA

24.1. A közérdekű és a közérdekből nyilvános adatok megismerhetőségét az Infotv. III. és IV. fejezetében foglaltakkal összhangban kell alkalmazni.

24.2. A Szervezet tevékenységével kapcsolatos adatok a közérdekből nem nyilvános személyes, a minősített, illetve az Infotv. egyéb törvény vagy európai uniós jogi aktus által más okból korlátozott adatok kivételével- közérdekűek, ezért ezekről a közvéleményt tájékoztatni kell. Az elutasított igényekről, valamint azok indokairól a Szervezet ügyviteli vezetője nyilvántartást vezet.

24.3. A Szervezet a közérdekű adatokat a Szervezet honlapján, a www.kamara.fogorvos.hu címen teszi közzé.

24.4. Az ügyviteli vezető a közzétételi listában nem szereplő közérdekű adatokra vonatkozó adatigénylések adataira tekintettel évente felülvizsgálja a Szervezet közzétételi listáját, és a jelentős arányban vagy mennyiségben felmerült adatigénylések alapján azt kiegészíti.

24.5. A Szervezet feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított 10 évig nem nyilvános. Ezen adatok megismerését – az adat megismeréséhez és a megismerhetőség kizárásához fűződő közérdek súlyát mérlegelve – az ügyviteli vezető engedélyezheti.

24.6. Jogszabály egyes adatok megismerhetőségének korlátozására az 11.4. bekezdésben meghatározottnál rövidebb időtartamot állapíthat meg.

25. A közérdekű adat megismerésére irányuló igény teljesítése

25.1. A közérdekű adat megismerése iránt bárki

- a) szóban [központi előterjesztési helyszín: Magyar Orvosi Kamara Fogorvosok Területi Szervezete, 1068 Budapest, Szondi u. 100. III. em.]),
- b) írásban (központi levelezési cím: Magyar Orvosi Kamara Fogorvosok Területi Szervezete, 1068 Budapest, Szondi u. 100. III. em.) vagy
- c) elektronikus úton (központi elektronikus levélcím: kamara@fogovos.hu , Hivatali Kapu: MOKFTESZ) a 4. melléklet szerint, vagy más módon igényt nyújthat be.

25.2. A közérdekű adat megismerésére irányuló igény esetén a Szervezet a tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül tesz eleget, ha annak feltételei fennállnak. Ez a határidő, ha az adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, egy alkalommal 15 nappal meghosszabbítható, erről az adatigénylőt az igény beérkezését követő 15 napon belül tájékoztatni kell.

25.3. A szóbeli kérelemről feljegyzést kell készíteni és az igénylőt lehetőleg már a kérelem előterjesztésekor nyilatkoztatni kell az adatszolgáltatás körülményekről és költségvonzatáról.

25.4. Az ügyviteli vezető a központilag előterjesztett igény alapján kijelöli – a szervezet munkamenetében megszokott módon, szóban vagy e-mail útján - az adatszolgáltatás teljesítésére köteles szervezeti egységet és annak ügyintézőjét. Eseti jelleggel az adatszolgáltatás teljesítését az ügyviteli vezető látja el.

25.5. A közérdekű adatok szolgáltatása kapcsán az ügyviteli vezető vagy az igénylő által megkeresett szervezeti egység vezetője, illetve ügyintézője a kérelmet – annak tartalma alapján – haladéktalanul köteles megvizsgálnia abból a szempontból, hogy

- a) az igényelt adatok pontosan beazonosíthatók-e,
- b) az igényelt adatokat a Magyar Orvosi Kamara Fogorvosok Területi Szervezete kezeli-e,
- c) az igényelt adatok közérdekű adatnak minősülnek-e,
- d) megtalálhatók-e a honlapon,
- e) a kért módon vannak-e tárolva a Magyar Orvosi Kamara Fogorvosok Területi Szervezeténél, vagy feldolgozásuk szükséges,
- f) a kérelmező elérhetősége tisztázott-e,
- g) a tájékoztatást milyen formában, módon kéri,
- h) az adatszolgáltatás teljesítése okoz-e a Szervezetnek költséget, illetve ennek megtérítését a kérelmező vállalja-e.

25.6. Ha a 11.5. bekezdésben meghatározott körülmények a kérelem alapján nem állapíthatók meg, az igénylőt meg kell keresni a hiányzó információkra vonatkozó nyilatkozata érdekében.

25.7. Ha a kért adatot nem a Szervezet kezeli, akkor a megkeresett szervezeti egység vezetője a kérelmet a lehető legrövidebb időn, de legfeljebb 8 napon belül továbbítja annak a szervnek, amelynek feladat- és hatáskörébe tartozik, és erről egyidejűleg tájékoztatja az igénylőt is. Ha a kért adatot a Szervezet, de nem a megkeresett szervezeti egység kezeli, akkor a megkeresett szervezeti egység vezetője a kérelmet a lehető legrövidebb időn, de legfeljebb 8 napon belül továbbítja annak a szervezeti egységnek, amelynek az adat kezelése a feladatkörébe tartozik.

25.8. Amennyiben olyan adat megismerésére irányul a kérelem, amelyet a Szervezet a honlapján már közzétett, – a fellelhetőséget is ideértve – az igénylőt erről tájékoztatni kell. Ez nem mentesíti a Szervezet az adatszolgáltatási kötelezettsége alól.

25.9. Az igény teljesítésének megtagadásáról és annak indokairól – jogorvoslati lehetőségek feltüntetésével – 15 napon belül a Szervezet levélben, vagy – amennyiben az igény elektronikus úton érkezett, illetve az igényben az elektronikus levelezési cím fel van tüntetve – elektronikusan tájékoztatást küld az igénylőnek.

25.10. Az igénylő a közérdekű adat megismerésére vonatkozó igény elutasítása vagy a teljesítésre nyitva álló (illetve a meghosszabbított) határidő eredménytelen eltelte esetén, valamint – ha a költségtérítést nem fizette meg – a másolat készítéséért megállapított költségtérítés összegének felülvizsgálata érdekében az illetékes járási/kerületi bíróságon keresettel élhet.

25.11. Az adatigénylő a közérdekű adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatos jogsértés esetén a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (www.naih.hu) is fordulhat.

26. Tájékoztatási kötelezettség teljesítése

26.1. A tájékoztatásnak – amennyiben az aránytalan költséggel nem jár – az igénylő által kívánt technikai eszközzel, illetve módon kell eleget tenni.

26.2. A Szervezet a kérelmeket az adatokba való betekintés lehetővé tételével is teljesítheti.

26.3. Betekintésre a Szervezet hivatali helyiségeiben, munkaidőben, az igénylővel előzetesen egyeztetett időpontban kerülhet sor. Betekintés esetén az igénylő az adatokról feljegyzést készíthet, illetve az adatokról másolatot kérhet. Ennek megtörténtéről az iratok közt feljegyzést kell készíteni.

26.4. Ha az igénylő szóbeli tájékoztatást kér, akkor ennek megtörténtéről az iratok közt feljegyzést kell készíteni.

26.5. Ha a közérdekű adatot tartalmazó dokumentum az igénylő által – jogszabály szerint – nem megismerhető adatot is tartalmaz, illetve más személy jogait a megismerés sértené, az igény teljesítése során ezen adatot felismerhetetlenné kell tenni.

26.6. Másolat készítésével, illetve azzal kapcsolatban felmerült, költség mértékéig térítés kérhető, melynek összegét előre közölni kell. A költségtérítés pontos összegét a Szervezet az adatszolgáltatást megelőzően köteles meghatározni.

26.7. Az igénylőtől egyértelmű nyilatkozatot kell kérni a tekintetben, hogy a költségek ismeretében fenntartja vagy módosítja kérelmét. Amennyiben a költségek megtérítését nem vállalja, közölni kell, hogy az igényelt adatokról csak olyan formában és módon kaphat tájékoztatást, ami nem okoz költséget a Szervezetnek.

26.8. Ha az igényelt dokumentum jelentős terjedelmű, a másolat iránti igényt a Szervezet a költségtérítés megfizetését követő 15 napon belül teljesíti. Erről az igénylőt az igény beérkezését követő 15 napon belül tájékoztatja.

26.9. A Szervezet a közzétett adatok megismerését személyazonosító adatok közléséhez nem kötheti. Az elektronikusan közzétett közérdekű adatokhoz történő hozzáférés biztosításához személyes adat csak annyiban kezelhető, amennyiben az technikailag elengedhetetlenül szükséges, a személyes adatokat ezt követően haladéktalanul törölni kell.

26.10. Az igénylő adatigényléshez kapcsolódó személyes adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez – beleértve az esetlegesen felmerülő költségek megfizetését is – elengedhetetlenül szükséges. Az igény teljesítését, illetőleg a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell.

26.11. A Szervezetet a közérdekű adat megismerésére irányuló kérelemnek az Info tv. rendelkezéseinek megfelelően tesz eleget.

26.12. Az adatszolgáltatási nyilvántartások az egyes szervezeti egységek vonatkozásában önállóan is vezethetők. A nyilvántartás egy másolati példányát – a tárgyévet követő év január 15. napjáig az ügyviteli vezető részére át kell adni.

26.13. Hiányos adatkérés esetén a hiány pótlására kell felkérni az adatkérőt. Nem kell hiánypótlást kérni, ha az adatkérés jogalapja, az adatszolgáltatás adattartalma e nélkül is megállapítható.

26.14. Az adatszolgáltatás feltételeit kétség esetén az adatkezelést végző ügyintéző vezetője, az ügyviteli vezető közreműködésével köteles ellenőrizni, mert az általa kezelt adatokért az érintettel szemben felelősséggel tartozik.

26.15. Abban az esetben, ha az adatszolgáltatást nem lehet jogszerűen teljesíteni, vagy az igény elbírálásához szükséges információkat az igénylő a felkérést követően sem jelölte meg, úgy az adattovábbítást meg kell tagadni.

26.16. Az adatszolgáltatás megtagadásáról – annak indokolásával együtt – írásban kell értesíteni az igénylőt.

26.17. Jelen szabályzat rendelkezéseit nem kell alkalmazni az összesített, illetve a statisztikai adatokra vonatkozó adatkérés esetén, amennyiben az adatfeldolgozás eredményeként az adatok elvesztik egyedi jellegüket.

V. ZÁRÓ RENDELKEZÉSEK

27.1. Jelen szabályzatban nem részletezett kérdések esetén a. vonatkozó jogszabályi rendelkezések irányadók. Jelen szabályzat az elfogadása napjától hatályos.

Magyar Orvosi Kamara
Fogorvosok Területi Szervezete
1068 Budapest, Szondi u. 100.
Telefon: +36-1-353-2188 Fax: +36-1-269-1876
E-mail: kamara@fogorvos.hu



Titoktartási kötelezettség vállalásáról szóló nyilatkozat

Alulírott

Név:

Anyja neve:

Születési hely és idő:

Cím:

Személyi azonosításra alkalmas igazolvány megnevezése és száma:

mint a Magyar Orvosi Kamara Fogorvosok Területi Szervezete (a továbbiakban MOK FTESZ)
.....(jogviszony minősítése) ezúton

n y i l a t k o z o m

arról, hogy az MOK FTESZ-nél ellátott tevékenységem során tudomásomra jutott, a közérdekű, illetve a közérdekből nyilvános adat fogalma alá nem tartozó adatokat, titkokat köteles vagyok megőrizni, azokat harmadik személy tudomására nem hozhatom.

Kötelezettséget válllok arra, hogy a tudomásomra jutott, fent jelzett információkkal kapcsolatban nyilatkozatot nem adok és azokat semmilyen formában nem használom fel, nyilvánosságra nem hozom.

Jelen titoktartási nyilatkozat aláírásával kijelentem, hogy a minősített- és személyes adatra, illetve az adó- és üzleti titokra vonatkozó jogszabályi rendelkezéseket megismertem és amennyiben munkavégzésem során a felsorolt adat, vagy titok jut tudomásomra, akkor azok tartalmának megismerését más részére nem teszem lehetővé.

Tudomásul veszem, hogy a titoktartási kötelezettség tevékenységem elvégzését, illetve a MOK FTESZ-szel fennálló jogviszonyom megszűnését követően is fennáll, továbbá, hogy fenti szabályok megsértése a hatályos anyagi- és eljárásjogi szabályok szerinti polgári jogi, és/vagy büntető jogi jogkövetkezményekkel jár.

Kelt:, 20... év. hónap ... nap.

.....

Aláírás

Készült: 2 példányban

Kapják: 1. számú példány: nyilatkozattevő

2. számú példány: irattár/személyi anyag

Magyar Orvosi Kamara
Fogorvosok Területi Szervezete
1068 Budapest, Szondi u. 100.
Telefon: 36-1-353-2188 Fax: +36-1-269-1876
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:

Személyi azonosításra alkalmas igazolvány megnevezése és száma:

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

HOZZÁJÁRULÁS KÜLÖNLEGES ADATOK KEZELÉSÉHEZ

Alulírott helység
..... közterület neve, jellege szám alatti lakos jelen
jognyilatkozat aláírásával hozzájárulok ahhoz, hogy a Magyar Orvosi Kamara Fogorvosok
Területi Szervezete

a számon folyamatban
lévő,

..... tárgyú
ügyben

a következő különleges adataimat feladatai ellátásával összefüggően kezelje:

1./

2./

3./

Az adatkezelés célja az alábbi (megfelelő aláhúzendő):

b) etikai eljárás lefolytatása

c) tagdíj kedvezmény megállapítása

d) egyéb:

Kijelentem, hogy a fenti adatszolgáltatás önkéntes, az erről, illetőleg az érintett
adatkezeléssel kapcsolatos jogaimról és jogorvoslati lehetőségekről szóló tájékoztatást
megkaptam.

Kelt. év hó nap.

.....
érintett

Ellenőrizve:

Kelt: év hó nap.

.....
adatvédelmi tisztviselő

KÖZÉRDEKŰ ADATSZOLGÁLTATÁSI NYILVÁNTARTÁS

Adatkezelő szervezet:

Adatkezelő működési minősége:

Időszak: év, hónap

Sorszám:

Adatkezelő nyilvántartási azonosítója:

Adatszolgáltatás ideje:

Adatszolgáltatás célja:

.....

.....

Adatkezelés jogalapja:

.....

.....

Adatszolgáltatást igénylő neve:

Szolgáltatott adatok köre:

.....

.....

Iktatószám:

A közérdekű adatszolgáltatási nyilvántartás fedőlapján kerülhet feltüntetésre a szervezeti egység neve, az adatszolgáltatási nyilvántartás megjelölés és a vezetésére felhatalmazó jogszabály megjelölése, a nyilvántartás vezetésének éve, a megnyitás időpontja, a vezető neve és aláírása, a nyilvántartás oldalainak oldalszáma összesen (számmal és betűvel feltüntetve).

Kelt:, év hó nap.

.....

Név:
ügyintéző/ szervezeti egység vezetője

Ellenőrizve:

Kelt:, év hó nap.

.....

ügyviteli vezető

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 elvesztése, 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 irodavezetőnek.
- 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 irodavezetőt. (Az adatfeldolgozóknak a „Megbízási szerződés adatfeldolgozó szempontú kiegészítése” című dokumentum által rögzített rendelkezéseket is be kell tartaniuk.)
- 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 rendelkezésre 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, irodavezetőt telefonon is értesíti. Ha a telefonos értesítési kísérlet sem jár sikerrel, a bejelentő az adatvédelmi tisztviselőt telefonon értesíti.

3. Az adatvédelmi tisztviselő által értesítendőkhöz 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 értesítendőkhöz 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 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.

A tudomásszerzés időpontjának az az időpont tekintendő, amikor az adatvédelmi tisztviselő az eseményt adatvédelmi incidensként minősíti.

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 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.